INNOBAND 6012-B1

User Manual

User Manual
Innoband 6012-B1

Manual Version 1.0
June 2012

Table of Contents

1. Product Introduction

1.1 Product Overview

Our INNOBAND 6012-B1 which complies with VDSL and VDSL2 standards is an VDSL terminal with one Ethernet port. It supports multiple network protocols and NAT Routing and Bridging functions. With stable performance, exquisite appearance and s great compatibility, it is the best choice for SOHO, small enterprise and individual users to access the Internet. By using the provided setup wizard, users can achieve fast installation without entering management interface.

1.2 Product Features

- Compliant to DSL Forum TR-048, TR-067 and TR-100 Interoperability Test
- Support bridge and router mode
- NAT/NAPT for sharing of a single DSL connection
- Comprehensive Firewall & Security Function
- Feature-Rich TR-069 supports Remote Registration / Remote Authentication / Remote Configuration
- Remote / Local configuration & management through Web / Telnet configuration & management
- Three levels access account management
- Device management access control based on source IP addresses and incoming interfaces
- System management includes SNMP, Telnet command line interface and web interface

1.3 System Requirement

In order to use, you must have the following:

- VDSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet network interface card (NIC) and/or a single computer with a USB port
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, Firefox v2.0 or later, or Netscape v6.1 or later

2. Hardware Description

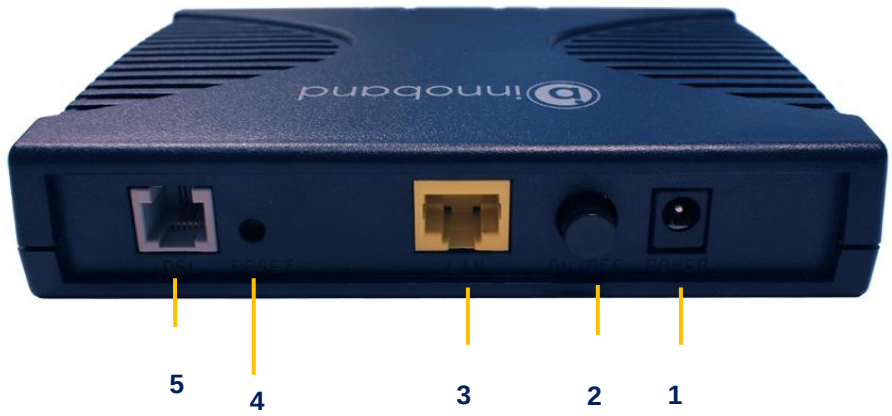
2.1 LED Description

The front panel contains lights called LEDs that indicate the status of the INNOBAND DSL.

LED	Color	Status	Description
POWER	Green	On	The device is power on.
		Off	The device is power off.
	Red	On	The device is booting up.
LAN	Green	On	The LAN port is connected to an powered Ethernet device.
		Blinking	The data is sending/receiving via LAN port.
		Off	The LAN port is not connected to any Ethernet device.
DSL	Green	On	The device is successfully linked with VDSL head-end.
		Slow Blinking	The device is trying to link with VDSL head-end.
		Fast Blinking	The device is handshaking with the VDSL head-end.
		Off	The device is not linked with VDSL head-end.
PPP/ACT	Green	On	The device is successfully connected to the Internet.
		Blinking	The device is sending/receiving data via the Internet.
		Off	The device is not connected to the Internet.
	Red	On	The device is failed to authenticate with the ISP due to username or password error.

2.2 Ports and Buttons

The rear panel contains the ports for the INNOBAND DSL's data and power connections.



1. **POWER:** Connecter for a power adapter. Using a power supply with a different voltage rating will damage this product. Make sure to observe the proper power requirements. The requirement of adapter is 12V/1A.

2. **ON/OFF:** Power switch to power on/off the INNOBAND DSL.

3. **LAN:** Connectors for Ethernet network devices, such as a PC, hub, switch or router.

4. **Reset:** Restore the device to the default settings.
You may need to restore the INNOBAND 6012-B1 to its factory defaults settings, after the configuration has changed and you lost the ability to enter the device via the web interface. To reset the INNOBAND DSL, simply press the reset button for 5-8 seconds. The device will be reset to its factory defaults. The reboot process will take about 30 seconds and the device will become operational again.

5. **DSL:** Connecter for accessing the Internet through VDSL line.

2.3 Installation Environment

2.3.1 Physical Environment Requirement

- Install the device horizontally
- Do not wipe the device with wet cloth
- Keep the device far away from hot objects
- Keep the environment clean and dry
- Power off the device and unplug the power adapter in lighting storm weather

2.3.2 Recommended Working Environment

- Temperature: 0˚ ~40˚
- Humidity: 10%~90% RH non-condensing

2.4 Hardware Installation

2.4.1 Installation Requirement

Before installing the device, make sure the following requirements are met.

1. Have enabled VDSL service and acquired at least one WAN IP address or user name and password provided by your ISP
2. One or more PCs with 10Base-T/100Base-T Network Adapter(s)
3. PC supporting Internet Explorer browser 6.0 or above

2.5 Installation Procedures

- Connect the Voice Splitter's Modem port to 6012-B1 Router's LINE port with telephone line (RJ11) and "Phone" port to a telephone. Insert a telephone line to the splitter's "Line" port.
- Connect one end of a network cable to 6012-B1' LAN (RJ45) port and the other end to PC's NIC.
- Plug the included power adapter into the Power socket on 6012-B1 Router and turn on the power switch.
- Check all connections as shown in the below figure to see if everything is ready.

3. Login to Web Management Interface

3.1 Configuring PC

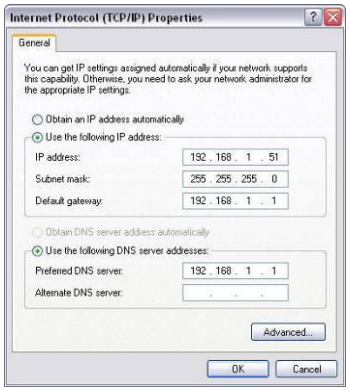
1. Right click “My Network Places” on the desktop and select “Properties”.

2. Right click “Local Area Connection” in the appearing window and select “Properties”.

3. Select “Internet Protocol (TCP/IP)” and click “Properties”.

4. Select “Obtain an IP address automatically” or “Use the following IP address”.
   a. “Obtain an IP address automatically” is shown in the figure below:

b. “Use the Following IP Address” is shown in the figure below:



IP address:
192.168.1.XXX：(XXX is any number from 2~254)

Subnet Mask:
255.255.255.0

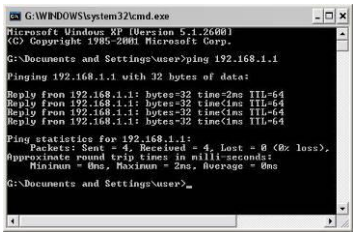
Gateway:
192.168.1.1

DNS server:
Enter your local DNS server address (consult your ISP if necessary). Or use the router as the DNS proxy server. Then click “OK” to submit and save the configurations.

3.2 Verifying Connection

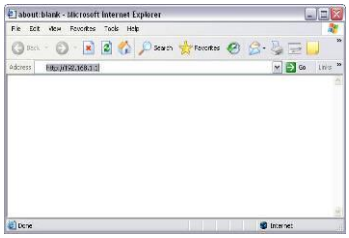
1. Select “Start”→All Programs”→“Accessories”→“Command Prompt”.

2. Input “ping 192.168.1.1” and press “Enter”. If the screen displays as shown in below figure, it means your PC is connected to your router successfully.



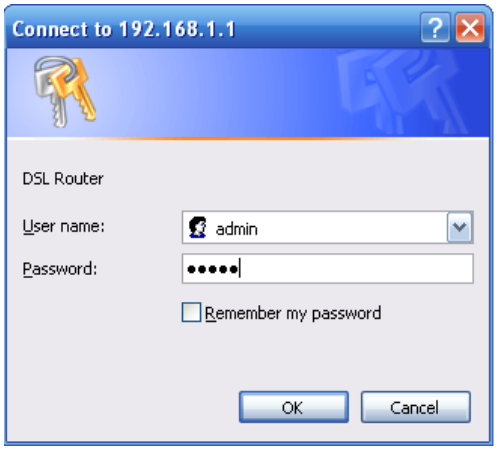
3.3 Login to Router

1. To access the router's Web-based interface, launch a web browser such as Internet Explorer and enter the Router's default IP address, http://192.168.1.1 and press "Enter".

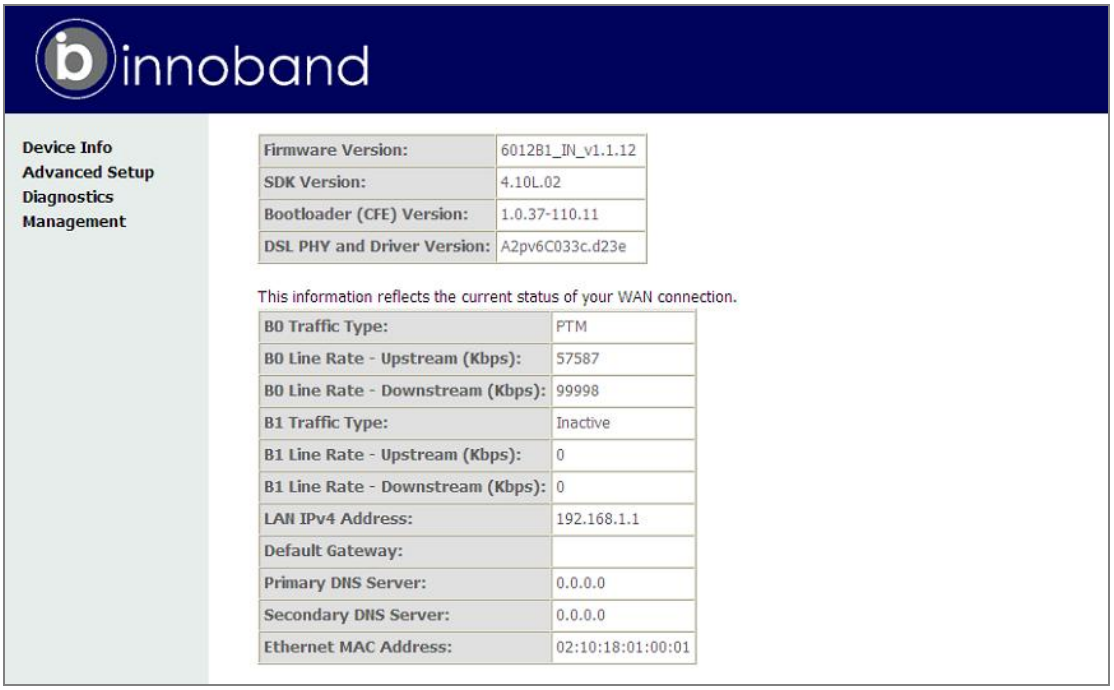


2. Input "admin" as both the "User Name" and "Password" and then click "OK" (Both user name and password are admin by default)

.

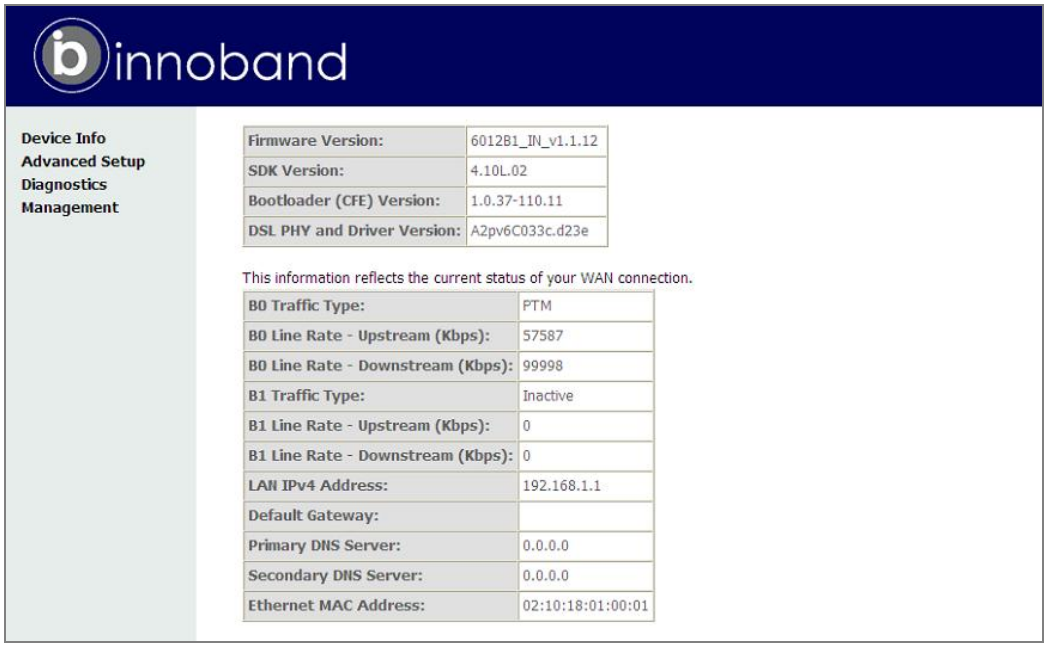


3. If you entered the correct user name and password, you will see the Page below.


innoband
Device Info
Advanced Setup
Diagnostics
Management
Firmware Version: 6012B1_IN_v1.1.12
SDK Version: 4.10L.02
Bootloader (CFE) Version: 1.0.37-110.11
DSL PHY and Driver Version: A2pv6C033c.d23e
This information reflects the current status of your WAN connection.
B0 Traffic Type: PTM
B0 Line Rate - Upstream (Kbps): 57587
B0 Line Rate - Downstream (Kbps): 99998
B1 Traffic Type: Inactive
B1 Line Rate - Upstream (Kbps): 0
B1 Line Rate - Downstream (Kbps): 0
LAN IPv4 Address: 192.168.1.1
Default Gateway:
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
Ethernet MAC Address: 02:10:18:01:00:01

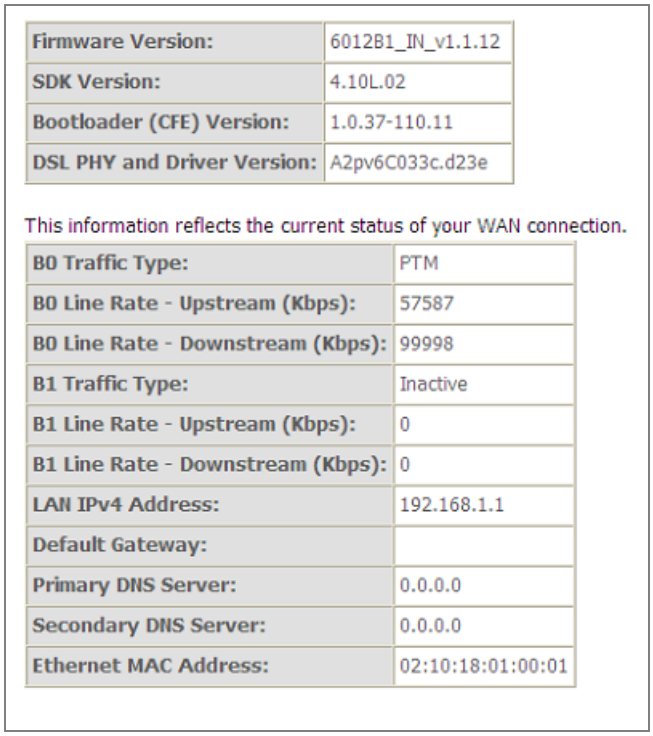
4. Quick Info in WEB GUI

This is the first page you see when entering the Web Application.



4.1 Summary

This page shows the status summary of the INNOBAND DSL



4.2 WAN

This page shows the WAN information of INNOBAND DSL.

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address	Action
atm0	br_0_0_35	Bridge	Disabled	Disabled	Disabled	Disabled	Unconfigured	0.0.0.0	
ptm0	br_0_0_1	Bridge	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0	

4.3 Statistics

This section shows the statistics information of INNOBAND.

4.3.1 LAN

This page shows the statistics of each connection on your LAN.

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	465620	3816	0	0	3198461	5732	0	0

Reset Statistics

4.3.2 WAN Service

This page shows the WAN statistics information.

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0	br_0_0_35	0	0	0	0	0	0	0	0
ptm0	br_0_0_1	143759	1213	0	0	139	139	0	0

Reset Statistics

4.3.3 xTM

This page shows the xTM interface statistics information.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	146960	21190	1239	139	0	0	0	0	0	0

Reset

4.3.4 xDSL

This page shows the DSL status and statistics.

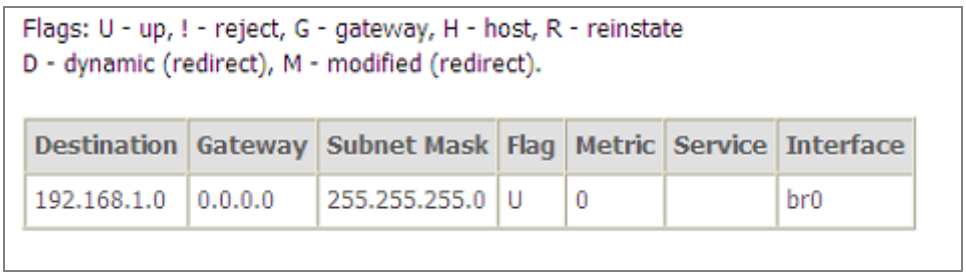
Statistics -- xDSL

Mode:		ADSL_2plus
Traffic Type:		ATM
Status:		Up
Link Power State:		L0
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	99	73
Attenuation (0.1 dB):	70	16
Output Power (0.1 dBm):	73	94
Attainable Rate (Kbps):	28472	1343
	Path 0	
	Downstream	Upstream
Rate (Kbps):	27419	1292
MSGc (# of bytes in overhead channel message):	51	13
B (# of bytes in Mux Data Frame):	244	13
M (# of Mux Data Frames in FEC Data Frame):	1	16
T (Mux Data Frames over sync bytes):	4	10
R (# of check bytes in FEC Data Frame):	0	8
S (ratio of FEC over PMD Data Frame length):	0.2856	5.5074
L (# of bits in PMD Data Frame):	6862	337
D (interleaver depth):	1	8
Delay (msec):	0.7	11.1
INP (DMT symbol):	0.0	0.75
Super Frames:	17003	16828
Super Frame Errors:	0	0
RS Words:	0	199727
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	7
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	17902338	291282978
Data Cells:	995	29600839
Bit Errors:	8	27806
Total ES:	12	0
Total SES:	11	0
Total UAS:	203	203

xDSL BER Test | Reset Statistics

4.4 Route

This page shows the IP route for INNOBAND DSL.

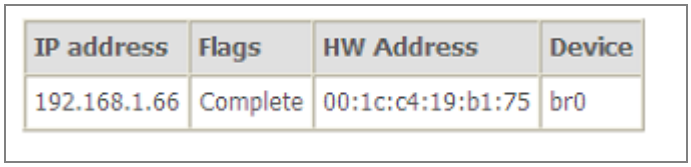


Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

4.5 ARP

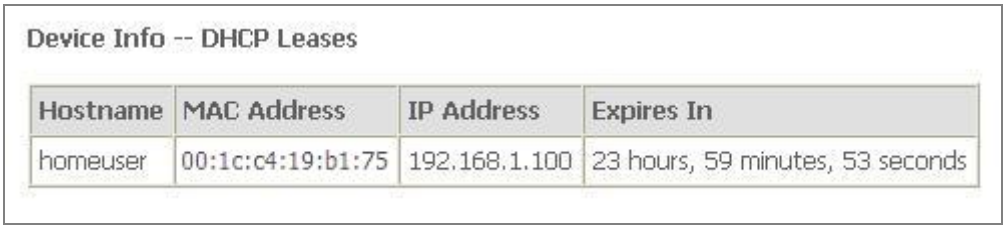
This page shows the ARP (Address Resolution Protocol) table on INNOBAND DSL.



IP address	Flags	HW Address	Device
192.168.1.66	Complete	00:1c:c4:19:b1:75	br0

4.6 DHCP

This page shows the client devices which are assigned IP addresses by the INNOBAND DSL.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
homeuser	00:1c:c4:19:b1:75	192.168.1.100	23 hours, 59 minutes, 53 seconds

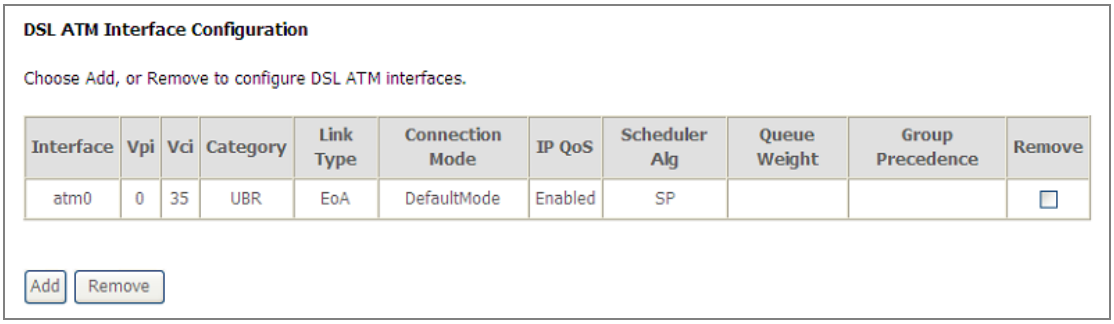
5. Advanced Setup

This section allows you to make specific configurations to your INNOBAND DSL such as NAT, Quality of Service, DNS and so on.

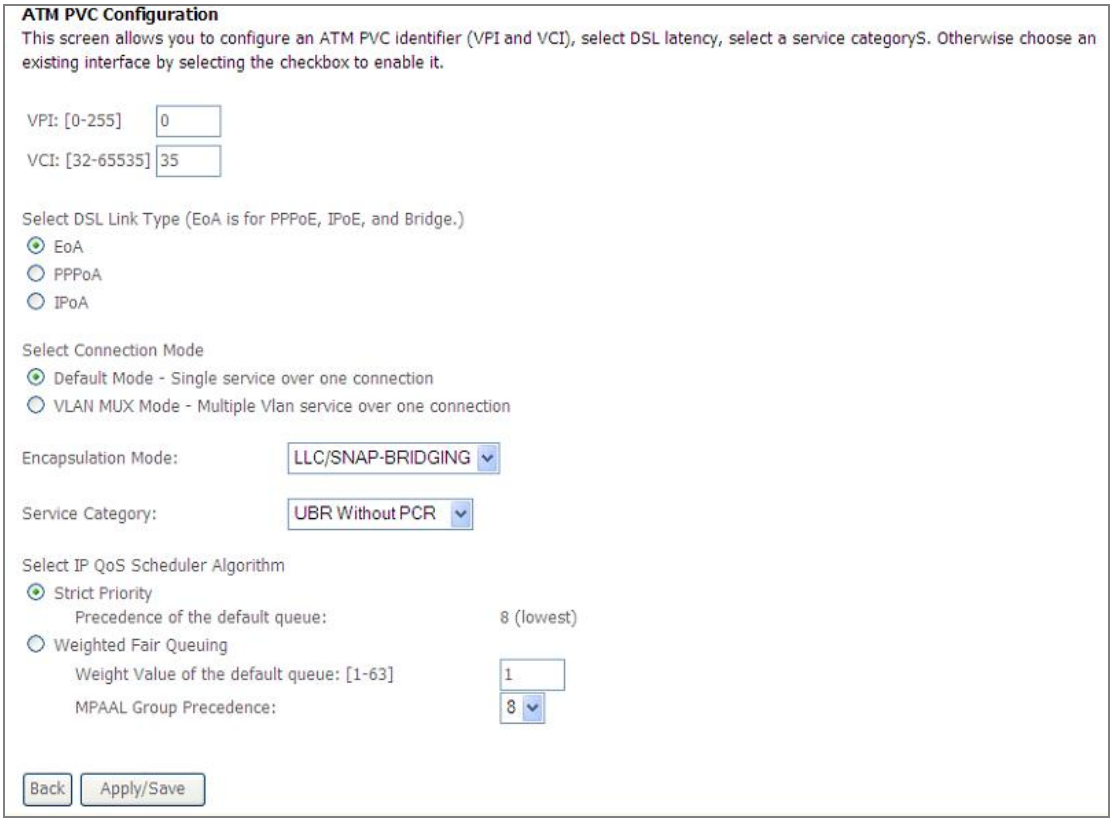
5.1 Layer2 Interface

5.1.1 ATM Interface

This page shows the summary of the current ATM interfaces you have configured. You can set up more than one connection profiles on your INNOBAND DSL.



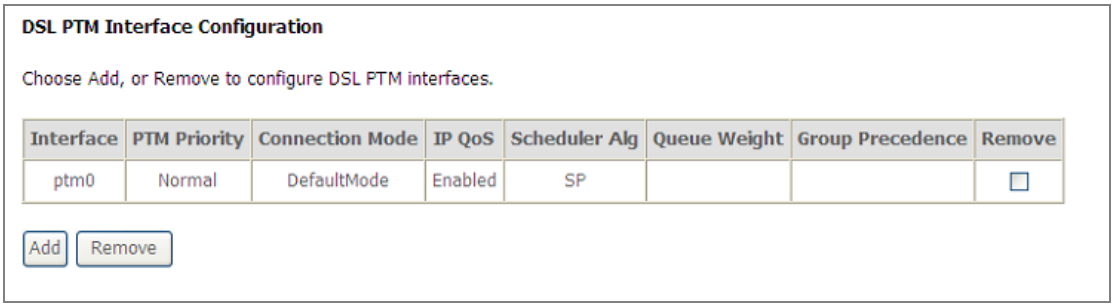
Click **Add** to create ATM interface. Enter the information provided by your ISP and then click **Save/Apply**.



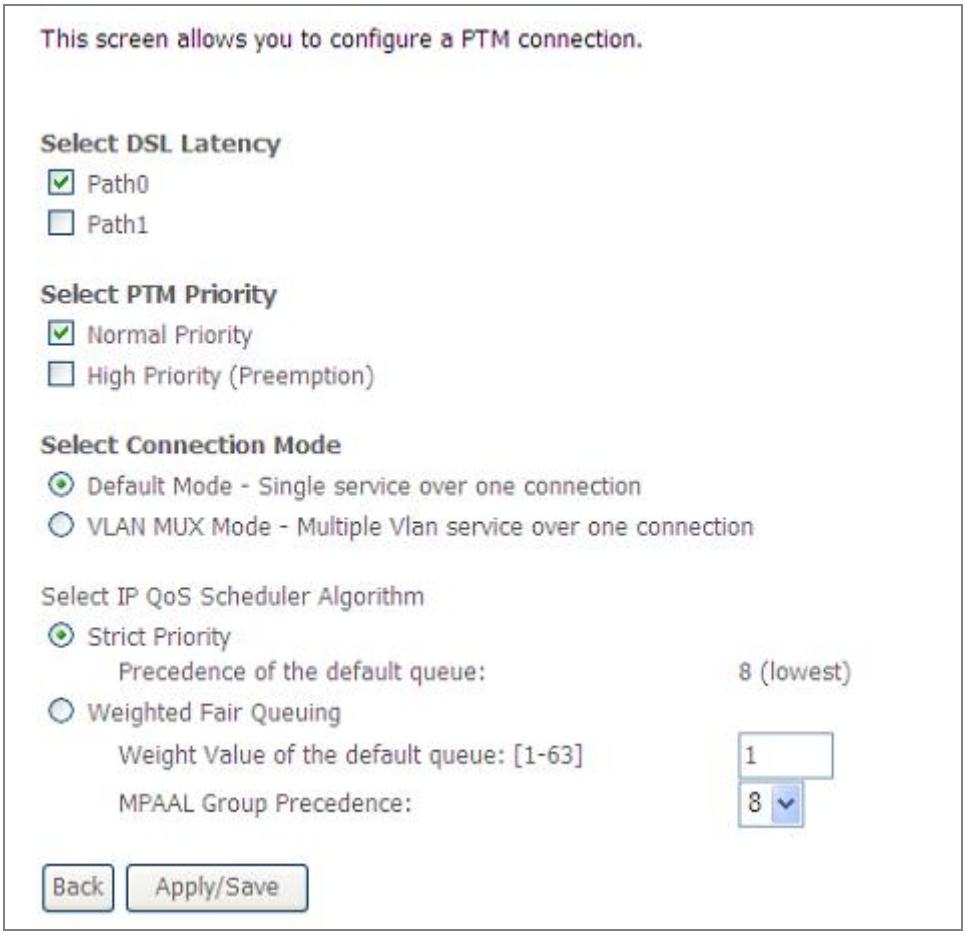
Field	Description
VPI/VCI	Enter the PVC identifier (VPI and VCI) provided by your ISP.
DSL Link Type	Select the DSL link type for the connection. Your ISP should inform you which type to use.
Encapsulation Mode	Select the encapsulation mode for the connection. Your ISP should inform you which mode to use.
Service Category	Select the encapsulation mode for the connection. If you are not sure which type to select, just use the default type.
Connection Mode	Select the connection mode according to your application.
Enable Quality of Service	Check to enable QoS feature. It improves the performance for selected classes of applications.

5.1.2 PTM Interface

This page shows the summary of the current PTM interfaces you have configured. You can set up more than one connection profiles on your INNOBAND DSL.



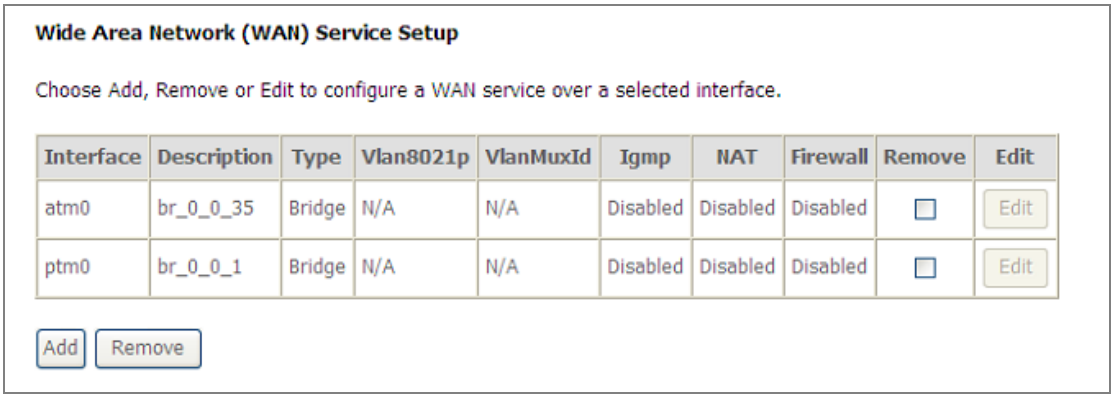
Click **Add** to create PTM interface. Enter the information provided by your ISP and then click **Save/Apply**.



Field	Description
PTM Priority	Select the **PTM priority** for the connection.
Connection Mode	Select the connection mode according to your application.
Enable Quality of Service	Check to enable QoS feature. It improves the performance for selected classes of applications.

5.2 WAN Service

This page shows the summary of the WAN service for a selected interface.



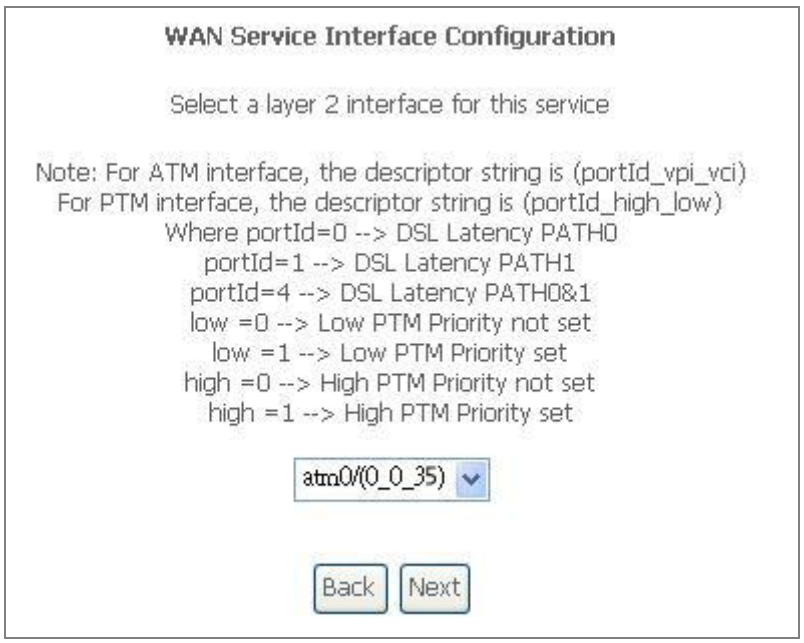
Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
atm0	br_0_0_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	☐	Edit
ptm0	br_0_0_1	Bridge	N/A	N/A	Disabled	Disabled	Disabled	☐	Edit

Add Remove

Click **Add** to configure WAN service. Select an interface from the drop-down list and click **Next**.



WAN Service Interface Configuration

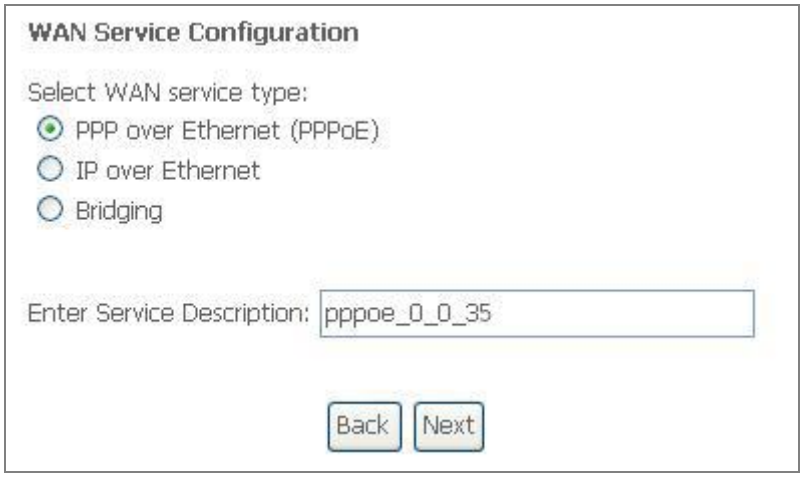
Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

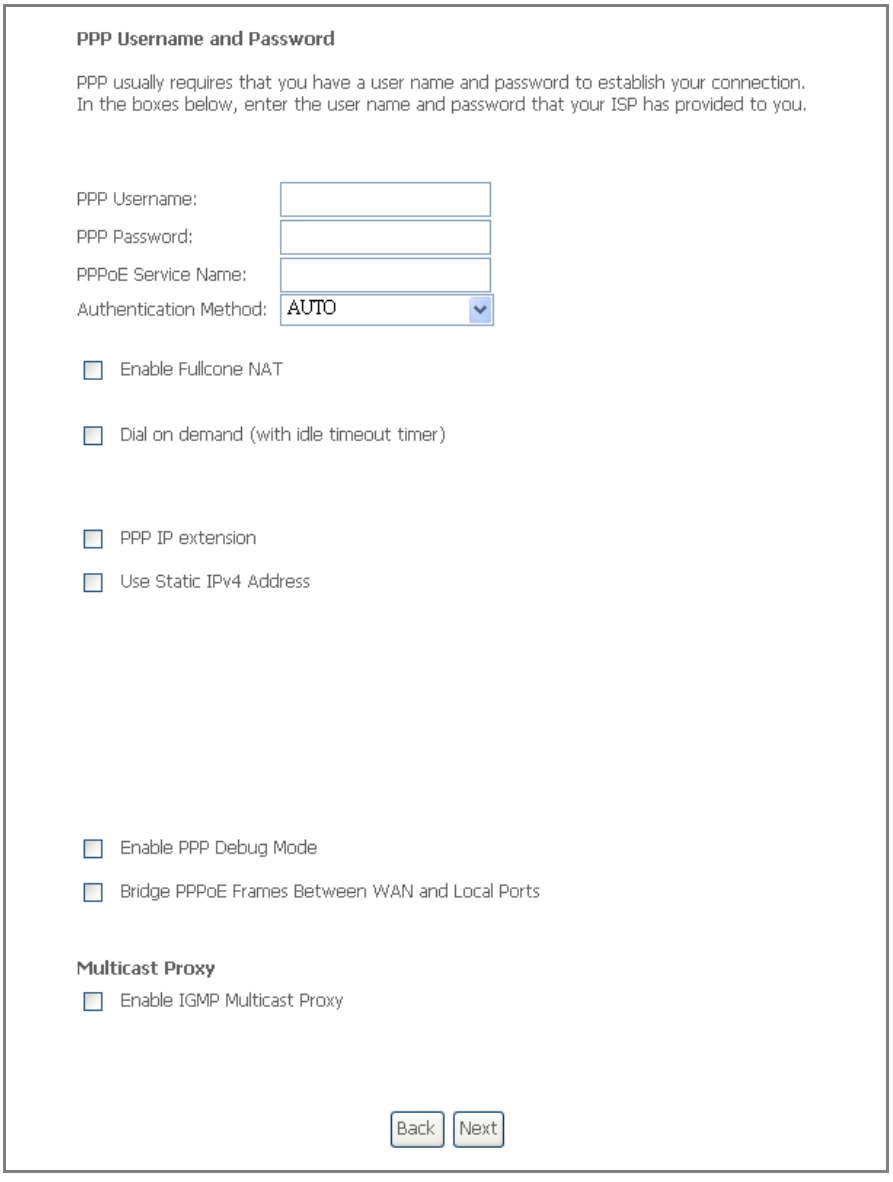
atm0/(0_0_35)

Back Next

Select a WAN service type and enter a service description for this connection. Different mode will lead you to different configuration page. Click **Next**.

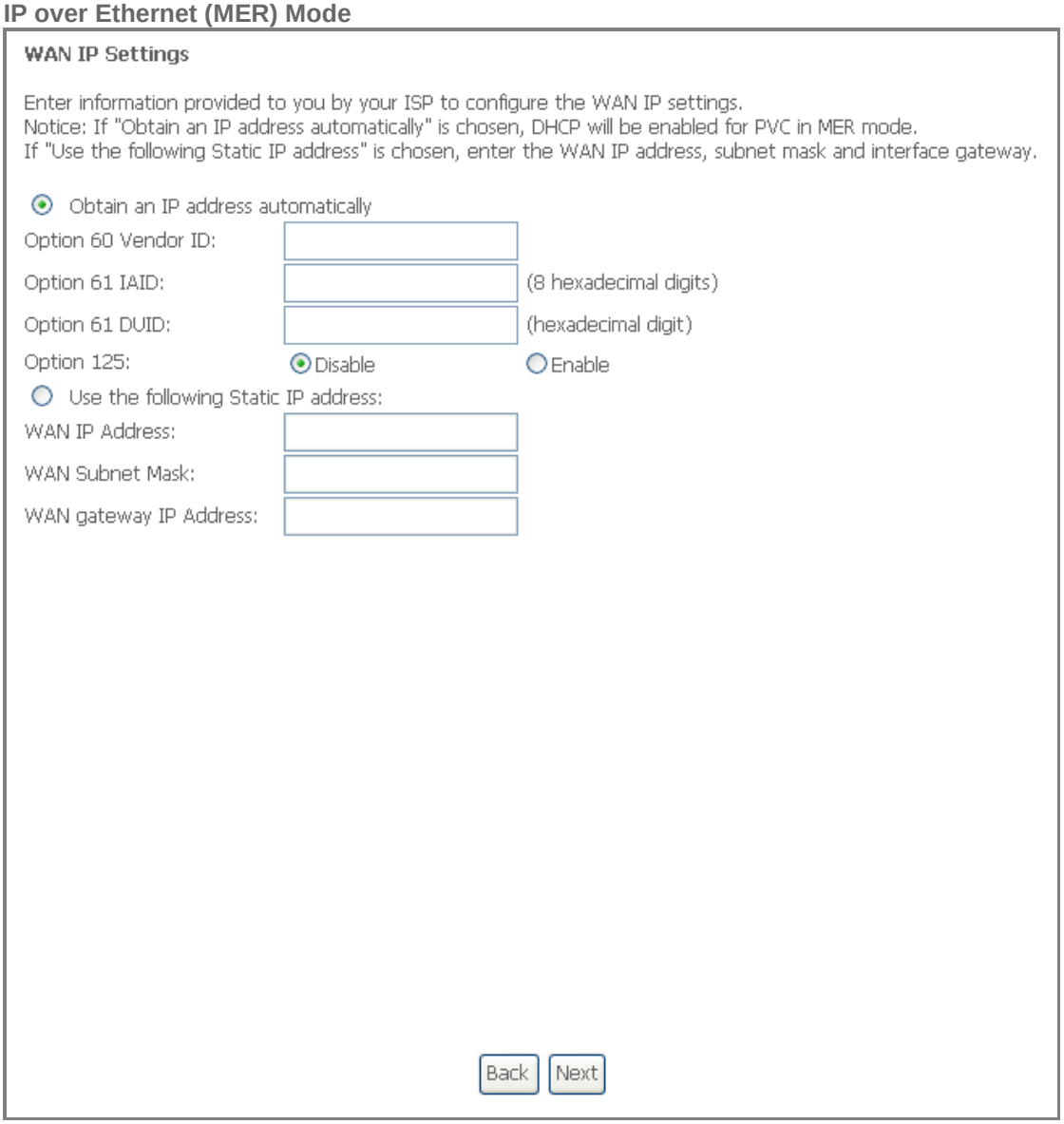


PPP over Ethernet (PPPoE) Mode



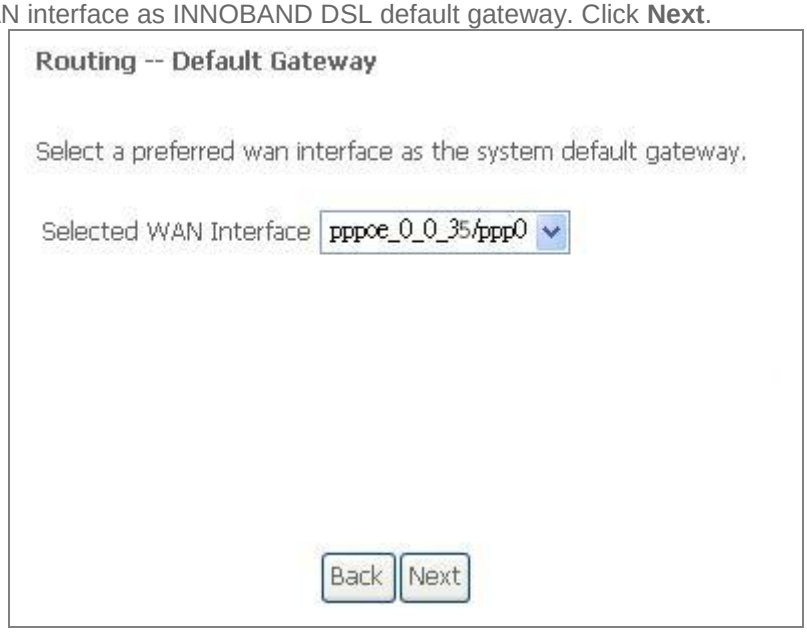
Field	Description
PPP Username	Enter the username of your PPP account.
PPP Password	Enter the password of your PPP account
PPPoE Service Name	Enter the service name if required by the ISP.
Authentication Method	Select the authentication method to be PAP, CHAP or MSCHAP. Select “Auto” to allow the INNOBAND DSL to negotiate with PPP server automatically.
Enable Fullcone NAT	Check to enable fullcone NAT feature.
Dial on Demand	Check to enable DOD feature.
Inactivity Timeout (minutes)	Specify the inactivity timeout (in minute) for DOD feature.
PPP IP Extension	Check to enable PPP IP extension.
Use Static IPv4 Address	Check and enter the static IPv4 address.
Enable PPP Debug Mode	Check to enable PPP debug mode.
Bridge PPPoE frames Between WAN and Local Ports	Check to enable the PPPoE fames bridging between WAN and Local Ports.
IGMP Multicast	Check to enable IGMP multicasting.

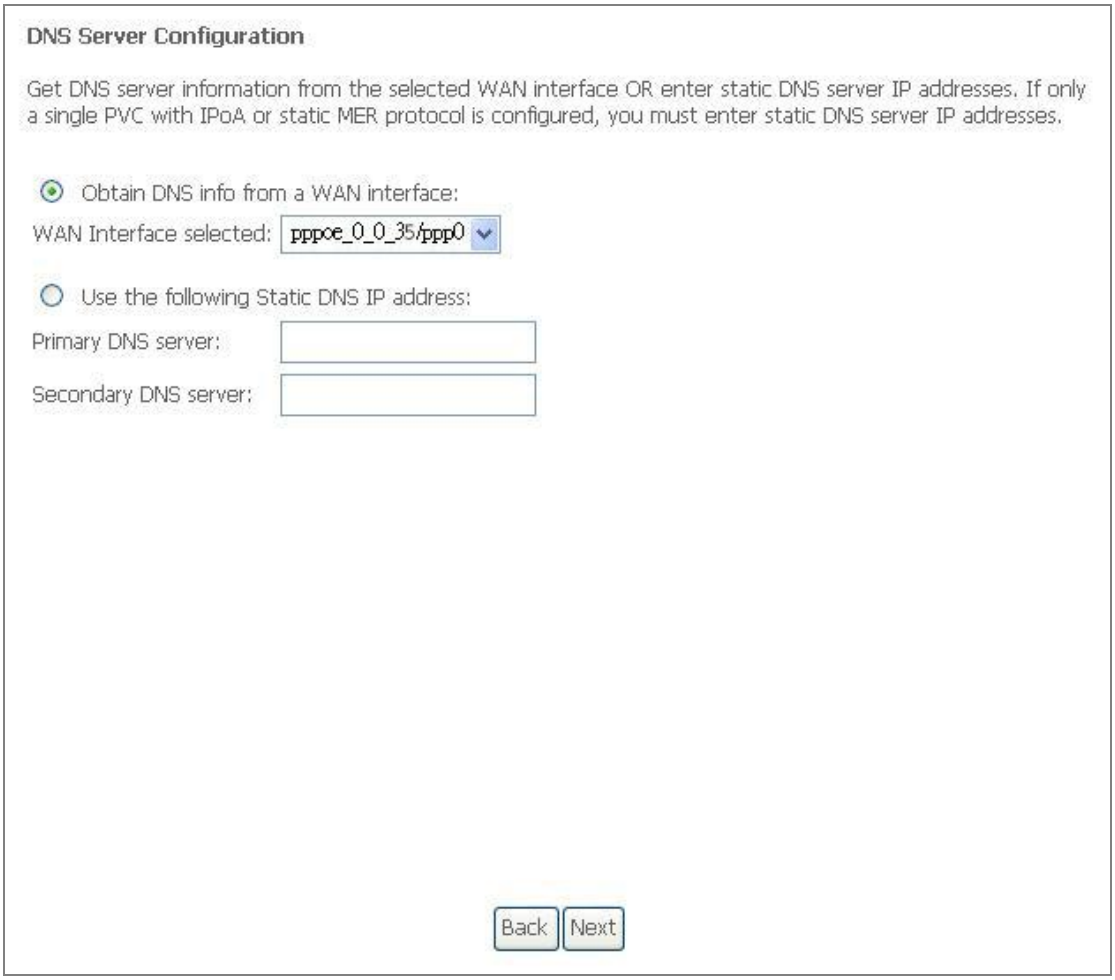
IP over Ethernet (MER) Mode



Field	Description
Obtain an IP Address Automatically	Select and select your preferred WAN interface from drop-down list. This allows the INNOBAND DSL to obtain the DNS server information automatically.
Option 60 Vendor ID	Your ISP will assign the Vendor Class IDentifier automatically. This option can be used by DHCP clients to identify the vendor and functionality of a DHCP client.
Option 61 IAID	Your ISP will assign the IAID (Identity Association IDentifier) automatically.
Option 61 DUID	Your ISP will assign the DUID (DHCP Unique IDentifier)) automatically.
Option 125	Select this item (Vendor-Identifying Vendor-Specific) to tell the INNOBAND DSL which firmware it has to download.
User the following Static IP Address	Select this mode and enter the static IP address, subnet mask and gateway IP address provided by your ISP.

Select a WAN interface as INNOBAND DSL default gateway. Click **Next**.





Field	Description
Obtain DNS Info from a WAN	Select the WAN interface to obtain the DSN info.
Use the Following Static DNS IP Address	Select to configure the static DNS IP address manually.
Primary DNS Sever	Enter the IP address of primary DNS server.
Secondary DNS Sever	(Optional) Enter the IP address of secondary DNS server.

The table below shows the summary of your WAN settings. Make sure they match the settings provided by your ISP so that you can connect to the Internet.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

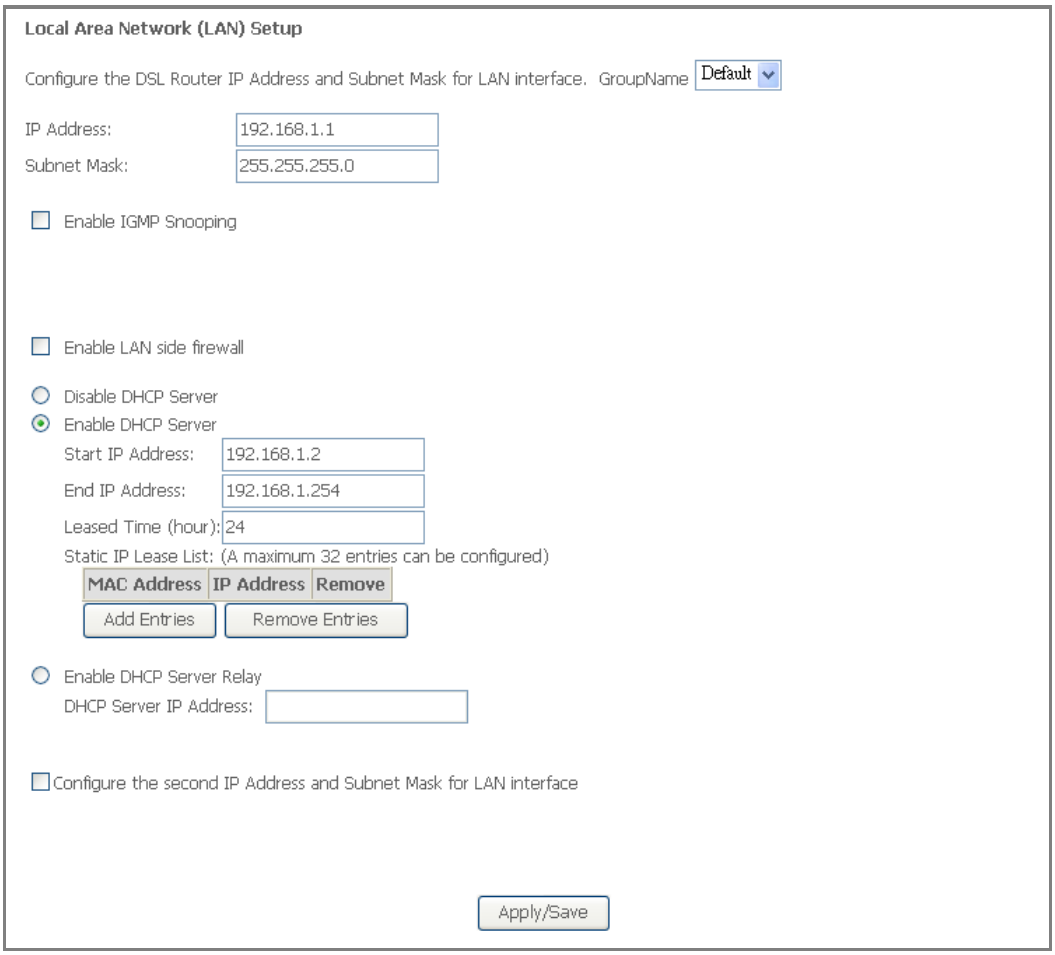
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

5.3 LAN

This page shows the current setting of LAN interface. You can set IP address/subnet mask and DHCP server pool for the LAN interface.



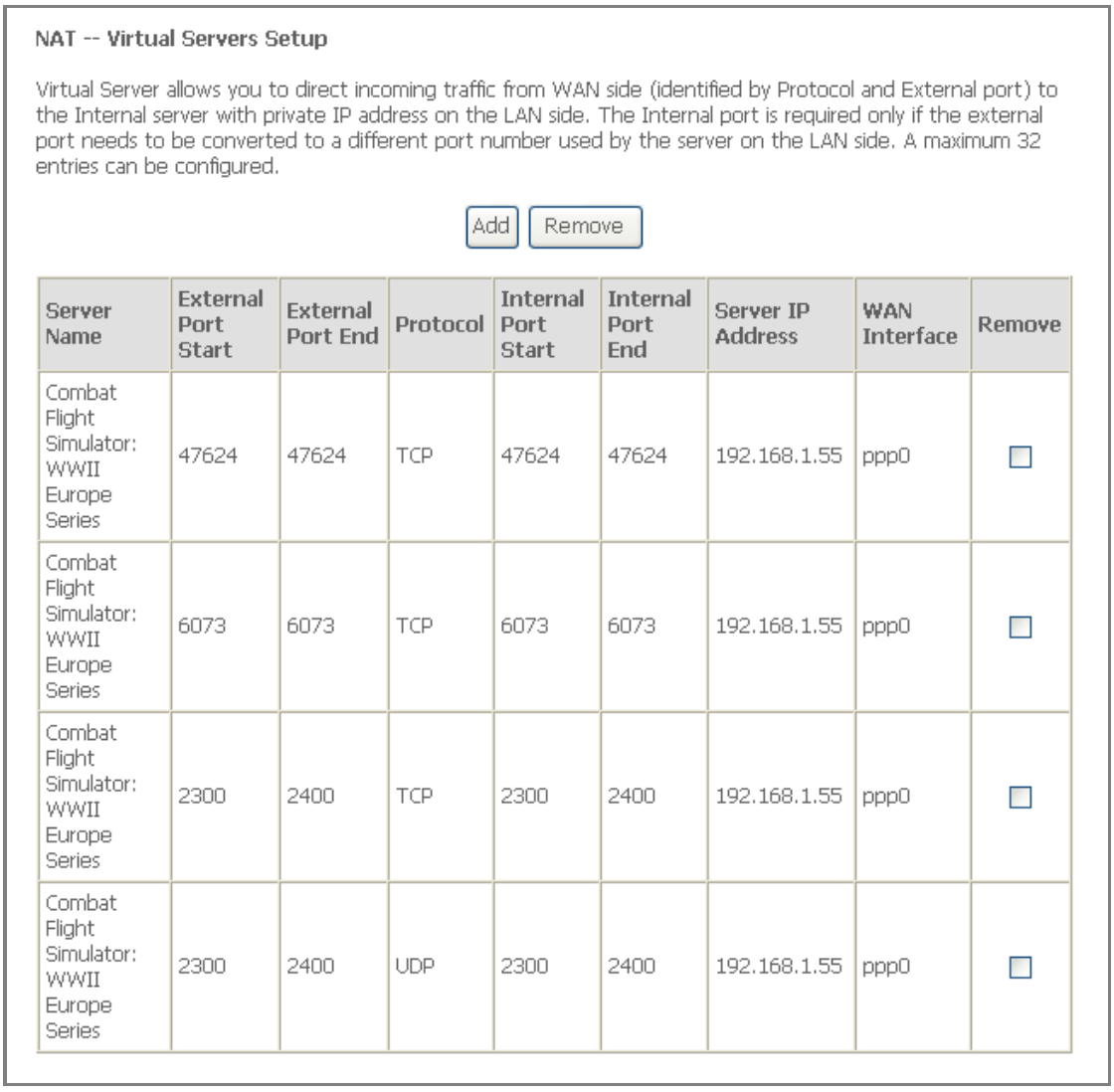
Field	Description
Group Name	Select a group name for this LAN.
IP Address	Enter the IP address for this LAN.
Subnet Mask	Enter the subnet mask for this LAN.
Enable IGMP Snooping	Check to enable IGMP Snooping and select the mode to be Standard or Blocking.
Enable LAN Side Firewall	Check to enable LAN side Firewall.
DHCP Server	If Enabled, the INNOBAND DSL will assign IP addresses to PCs (DHCP clients) on your LAN when they start up. The default setting is Enabled.
Start/End IP Address	Configure the DHCP range used by the DHCP server when assigning IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.
Leased Time (hour)	Configure the amount of time the clients will be allowed to connect to DHCP server. If set to 0, the allocated IP addresses will be effective forever.
Static IP Leased Time	Click Add Entries to configure static LAN IP according to its MAC address to the clients.

Second IP Address	Enter the second IP address for this LAN if needed.
Subnet Mask	Enter the subnet mask for this LAN.

5.4 NAT

5.4.1 Virtual Servers

You can configure the INNOBAND DSL as a virtual server. Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.



NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Combat Flight Simulator: WWII Europe Series	47624	47624	TCP	47624	47624	192.168.1.55	ppp0	☐
Combat Flight Simulator: WWII Europe Series	6073	6073	TCP	6073	6073	192.168.1.55	ppp0	☐
Combat Flight Simulator: WWII Europe Series	2300	2400	TCP	2300	2400	192.168.1.55	ppp0	☐
Combat Flight Simulator: WWII Europe Series	2300	2400	UDP	2300	2400	192.168.1.55	ppp0	☐

Click **Add** to configure virtual server. Select the virtual server from the drop-down list or custom the service you need. Then complete the server IP address and click the **Apply/Save**.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**
Remaining number of entries that can be configured:32

Use Interface: pppoe_0_0_35/ppp0

Service Name:

- (•) Select a Service:
- ( ) Custom Service:

Server IP Address: 192.168.1.55

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
47624	47624	TCP	47624	47624
6073	6073	TCP	6073	6073
2300	2400	TCP	2300	2400
2300	2400	UDP	2300	2400
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Apply/Save

5.4.2 Port Triggering

Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, require that specific ports in the Router's firewall be opened for access by the remote parties.
Port Trigger dynamically opens up the “Open Ports” in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the “Triggering Ports”. The INNOBAND DSL allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the ”Open Ports”. A maximum 32 entries can be configured.

NAT -- Port Triggering Setup

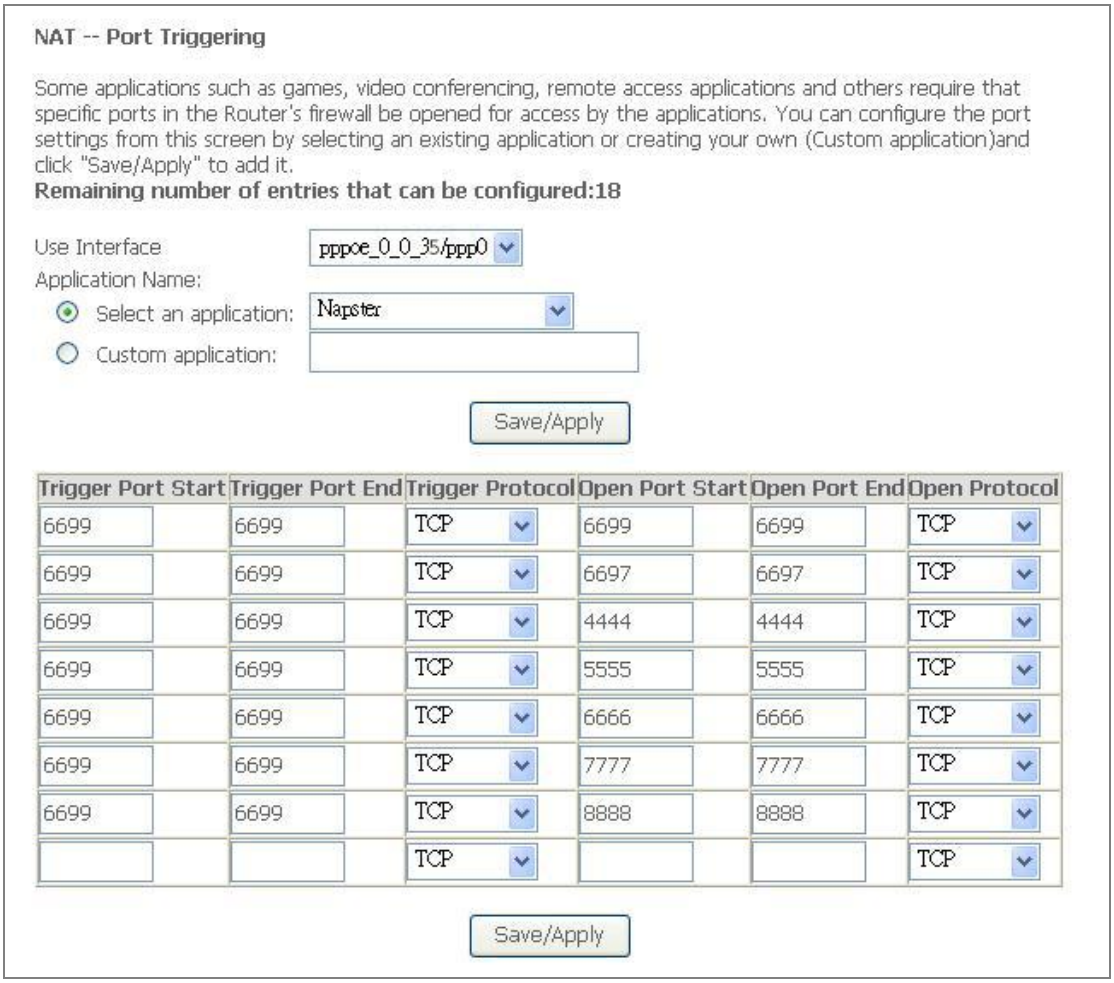
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Add Remove

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
Napster	TCP	6699	6699	TCP	6699	6699	ppp0	☐
Napster	TCP	6699	6699	TCP	6697	6697	ppp0	☐
Napster	TCP	6699	6699	TCP	4444	4444	ppp0	☐
Napster	TCP	6699	6699	TCP	5555	5555	ppp0	☐
Napster	TCP	6699	6699	TCP	6666	6666	ppp0	☐
Napster	TCP	6699	6699	TCP	7777	7777	ppp0	☐
Napster	TCP	6699	6699	TCP	8888	8888	ppp0	☐

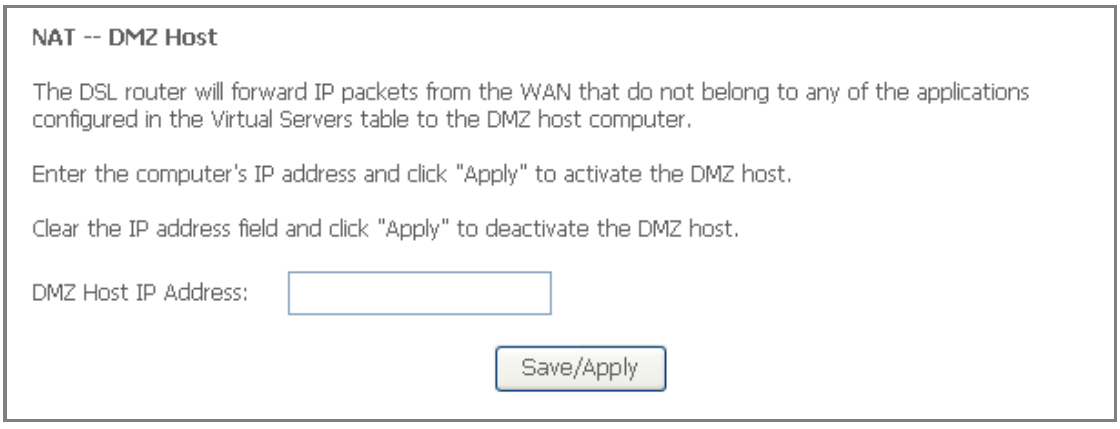
Add Remove

Click **Add** to configure the Port Triggering. Select the applications that you want to set up the port settings and then click **Save/Apply**.



5.4.3 DMZ Host

The INNOBAND DSL can forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

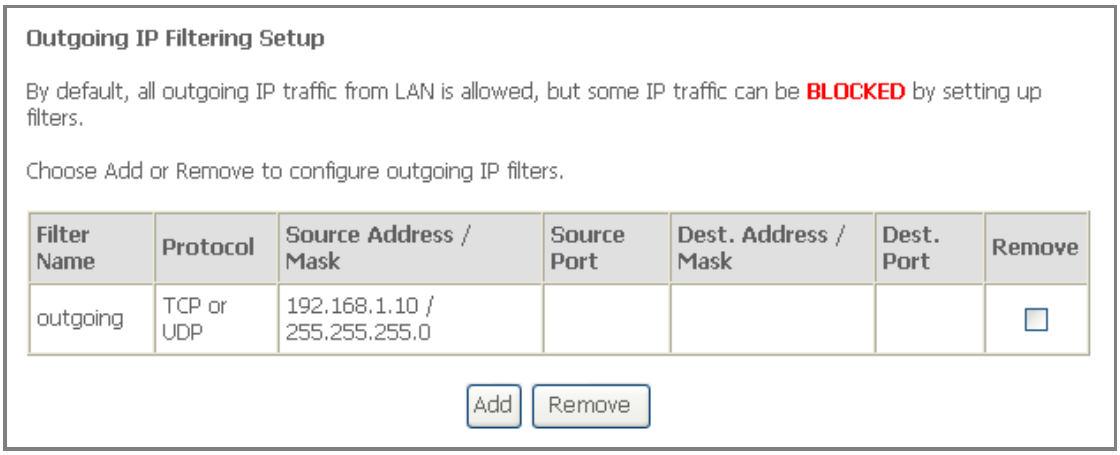


To activate the DMZ host, enter the computer's IP address and click **Save/Apply**. To deactivate the DMZ host, clear the IP address field and click **Save/Apply**.

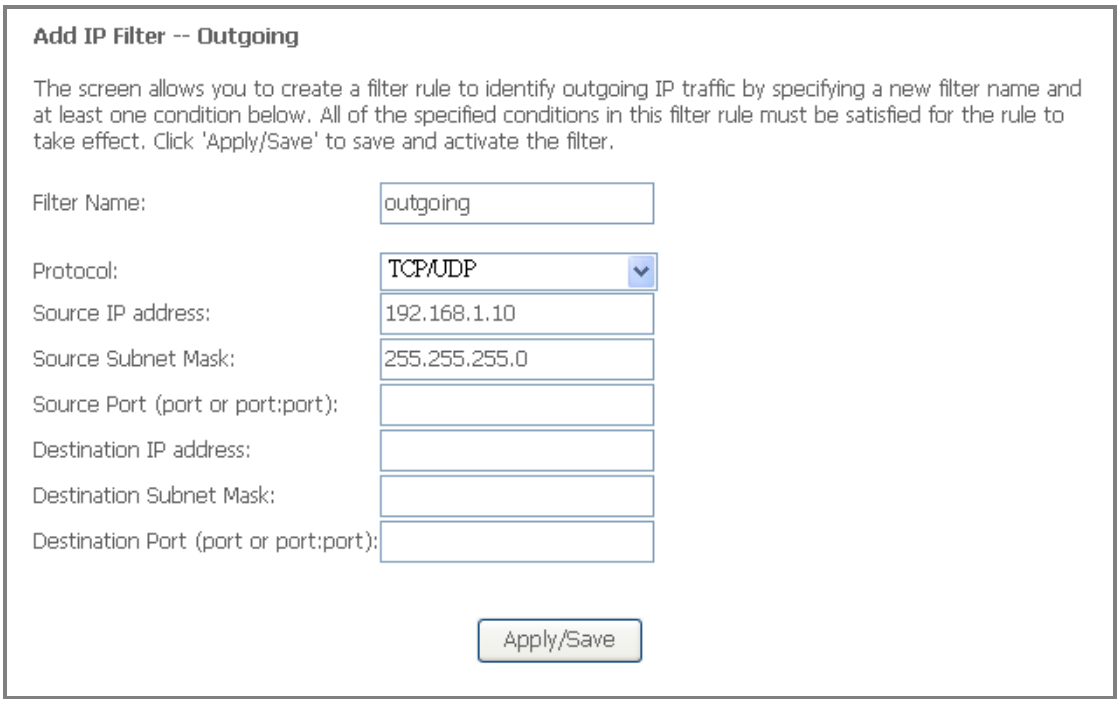
5.5 Security – IP Filtering

5.5.1 Outgoing

The outgoing filter blocks the LAN traffic from entering the WAN side. By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.



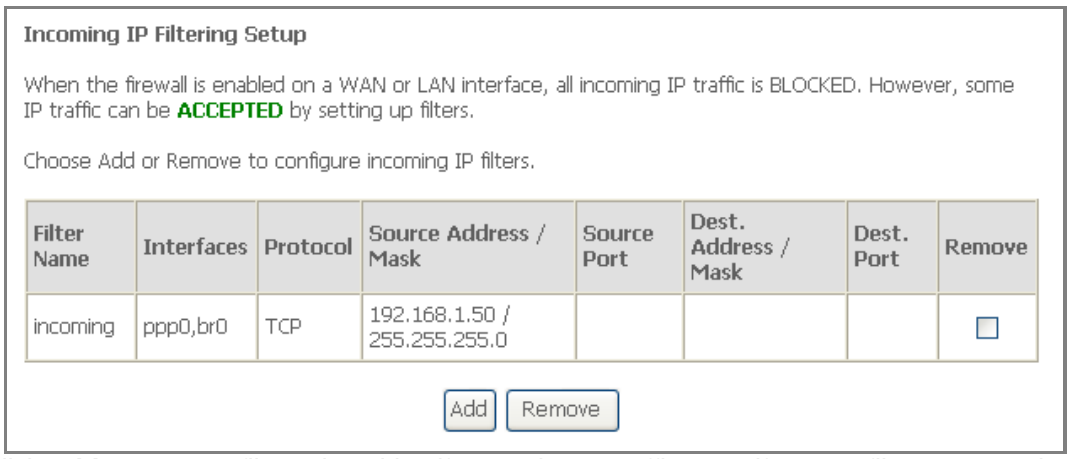
Click **Add** to create a filter rule to identify outgoing IP traffic. Specify a new filter name and at least one condition. Then click **Save/Apply**. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.



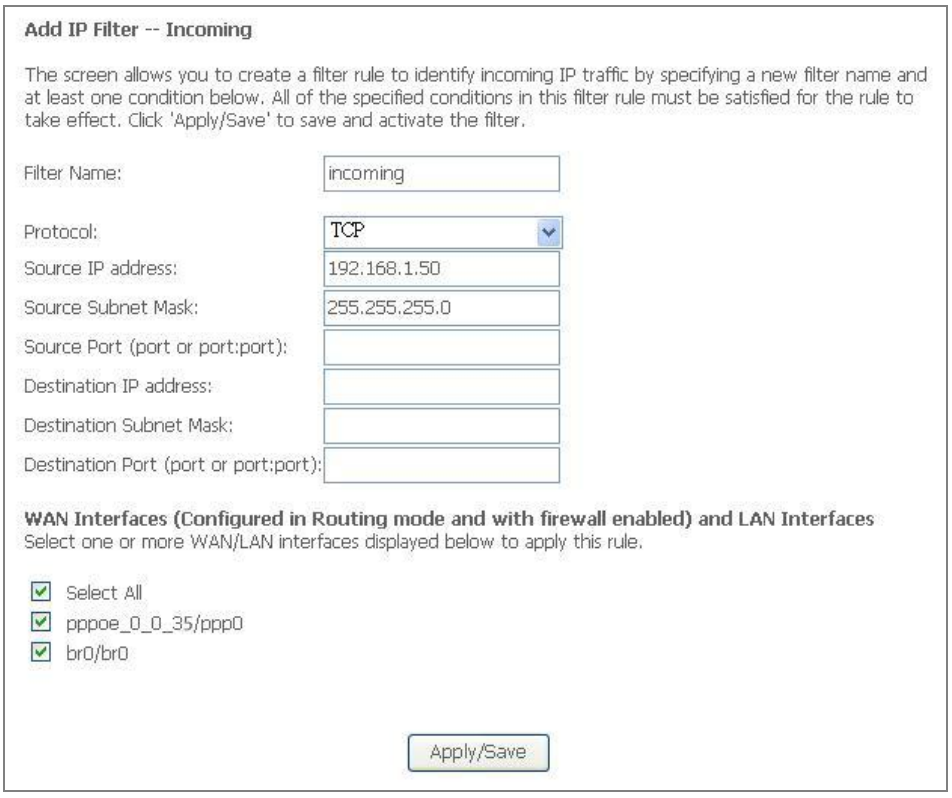
Field	Description
Filter Name	Enter a name for this filter rule.
Protocol	Select the protocol to be used from the drop-down list.
Source IP Address / Subnet Mask/ Port	Enter the source (from the LAN side) IP address, subnet mask and port number.
Destination IP Address / Subnet Mask / Port	Enter the destination (from the WAN side) IP address, subnet mask and port number.

5.5.2 Incoming

Incoming IP filter filters the WAN traffic to the LAN side. When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is blocked. This page allows you to configure filters for accepting some incoming IP traffic.



Click **Add** to create a filter rule to identify outgoing IP traffic. Specify a new filter name and at least one condition. Then click **Save/Apply**. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.



Field	Description
Filter Name	Enter a name for this filter rule.
Protocol	Select the protocol to be used from the drop-down list.
Source IP Address / Subnet Mask/ Port	Enter the source (from the WAN side) IP address, subnet mask and port number.
Destination IP Address / Subnet Mask / Port	Enter the destination (from the LAN side) IP address, subnet mask and port number.
WAN/LAN Interface	Select the WAN and LAN interface to apply this rule.

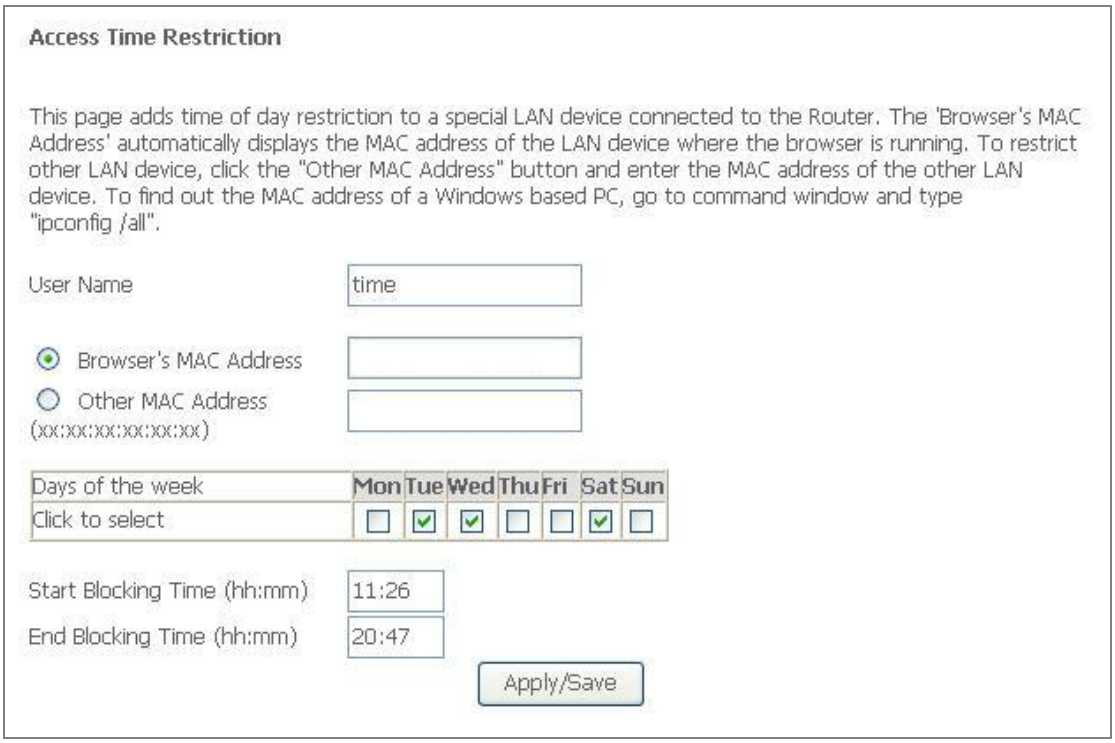
5.6 Parental Control

Parental Control allows you to add the day of the week and URL restrictions to specific LAN clients.

5.6.1 Time Restriction

This page allows you to block Internet access from specified LAN clients for specified periods. Make sure that either the system time is specified directly or Internet time server is configured.

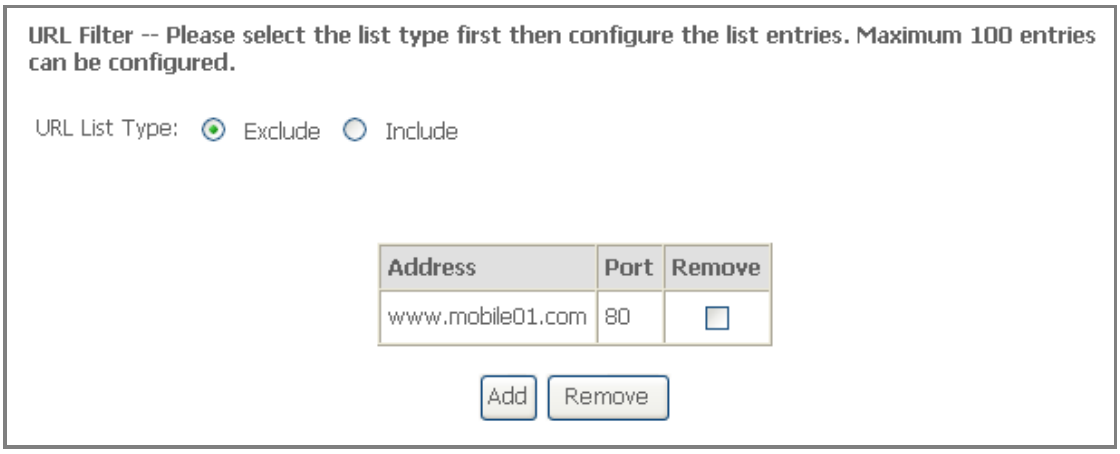
Click **Add** to configure the restriction. Enter the settings and then click **Save/Apply**.



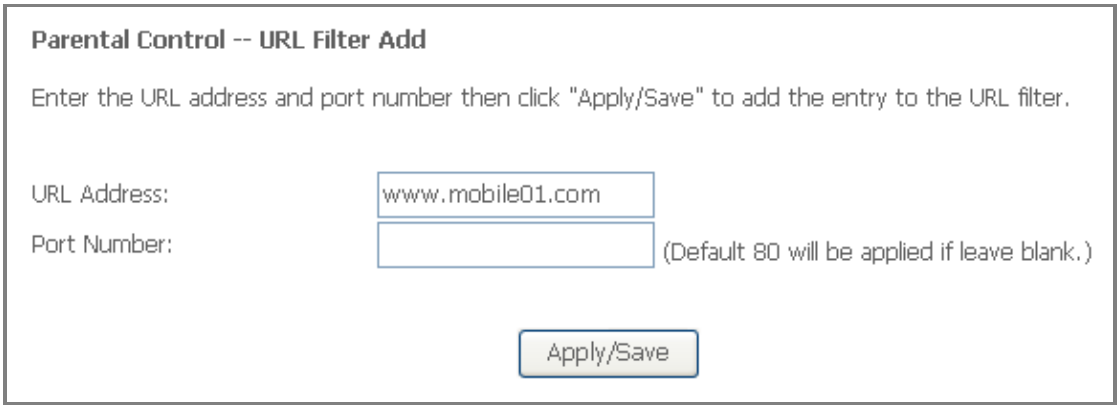
Field	Description
User Name	Enter a name for this restriction.
Browser's MAC Address	This is the MAC address of the LAN device where the browser is running.
Other MAC Address	Select and enter other LAN device's MAC address.
Select Days of the Week	Check the days of the week of blocking.
Start/End Blocking Time	Enter the start and end time of blocking.

5.6.2 URL Filter

This page allows you to block specified URLs from accessing. Maximum 100 entries can be configured.



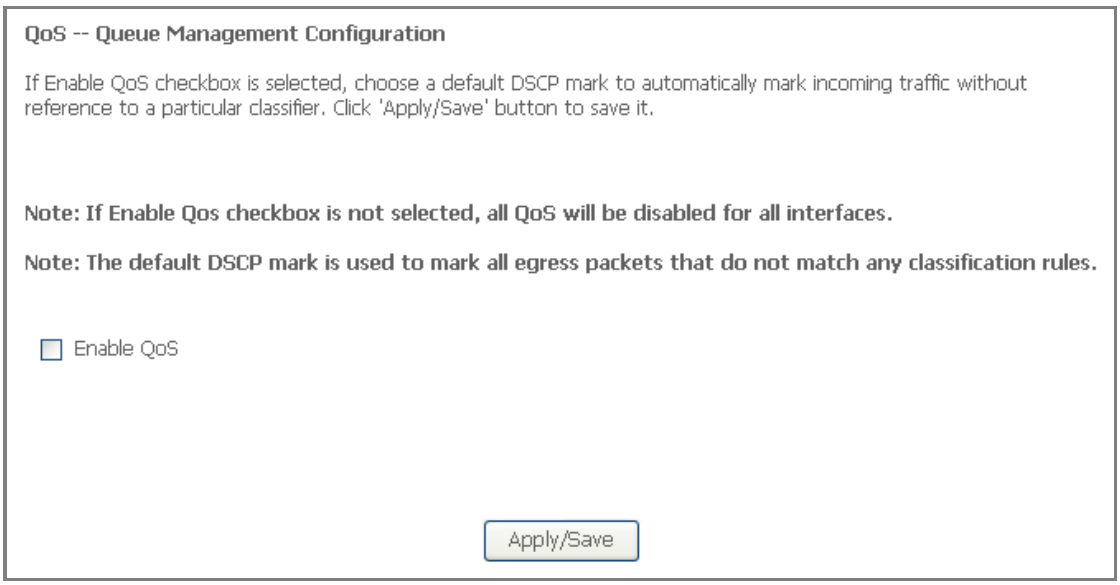
Select the list type first and then click **Add** to configure the URL entries. Enter the URL address and port number. Then click **Save/Apply**.



Field	Description
URL Address	Enter the URL address of blocking.
Port Number	Enter the port number of blocking.

5.7 Quality of Service

You can configure the Quality of Service to apply different priorities to traffic on the INNOBAND DSL. If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

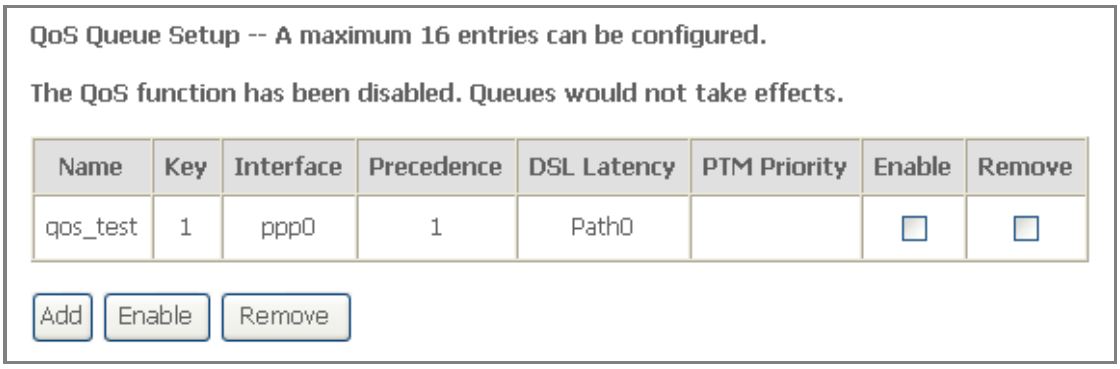


To enable QoS, check **Enable QoS** checkbox and select a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Then click **Save/Apply**.

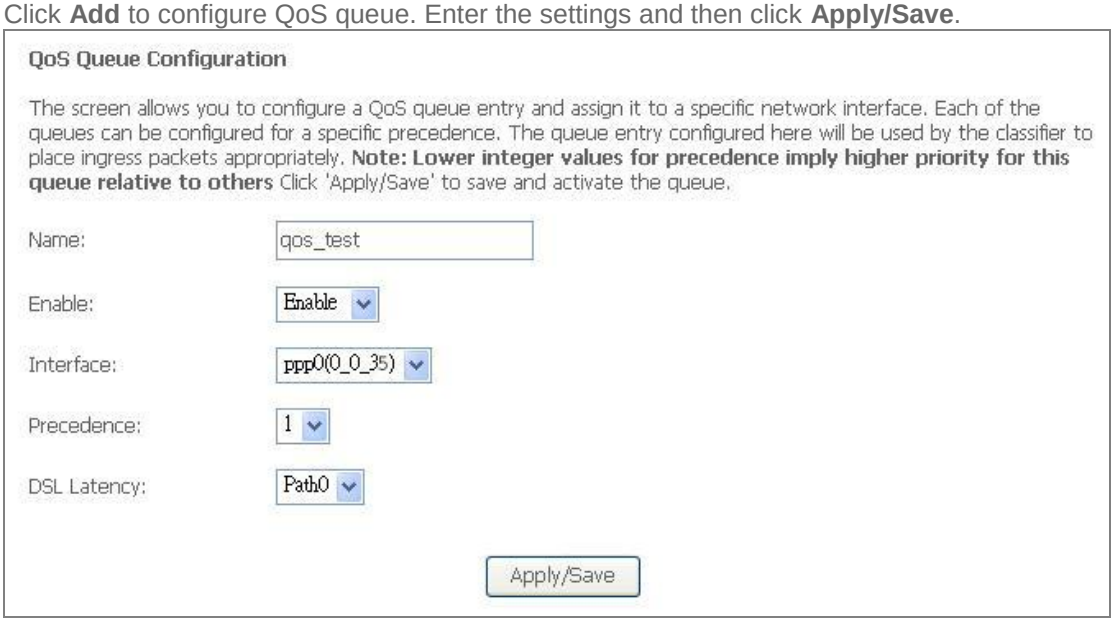
Field	Description
Select Default DSCP Mark	Select the DSCP mark to mark all egress packets that do not match any classification rules.

5.7.1 Queue Config

This page shows the QoS queue on the INNOBAND DSL. The Queue configuration allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. If you disable WMM function in Wireless Page, queues related to wireless will not take effects



Click **Add** to configure QoS queue. Enter the settings and then click **Apply/Save**.



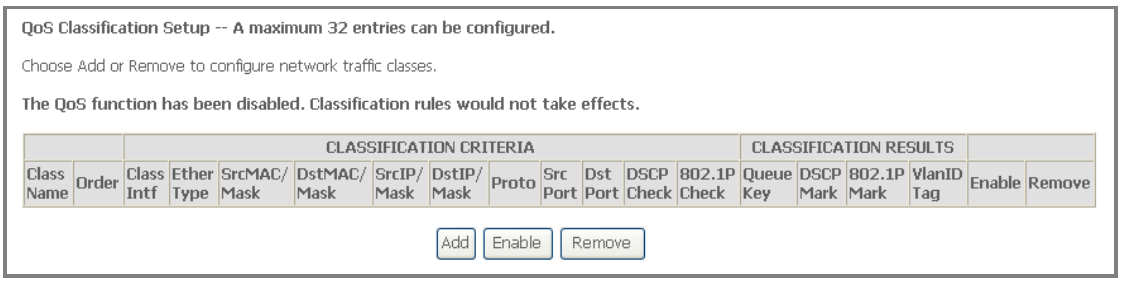
Field	Description
Name	Enter a name for the queue.
Enable	Select to enable or disable this queue.
Interface	Select an interface for this queue to apply.
Precedence	Select the precedence for this queue. Lower integer values imply higher priority for this queue relative to others.

Below is the table of precedence summary:

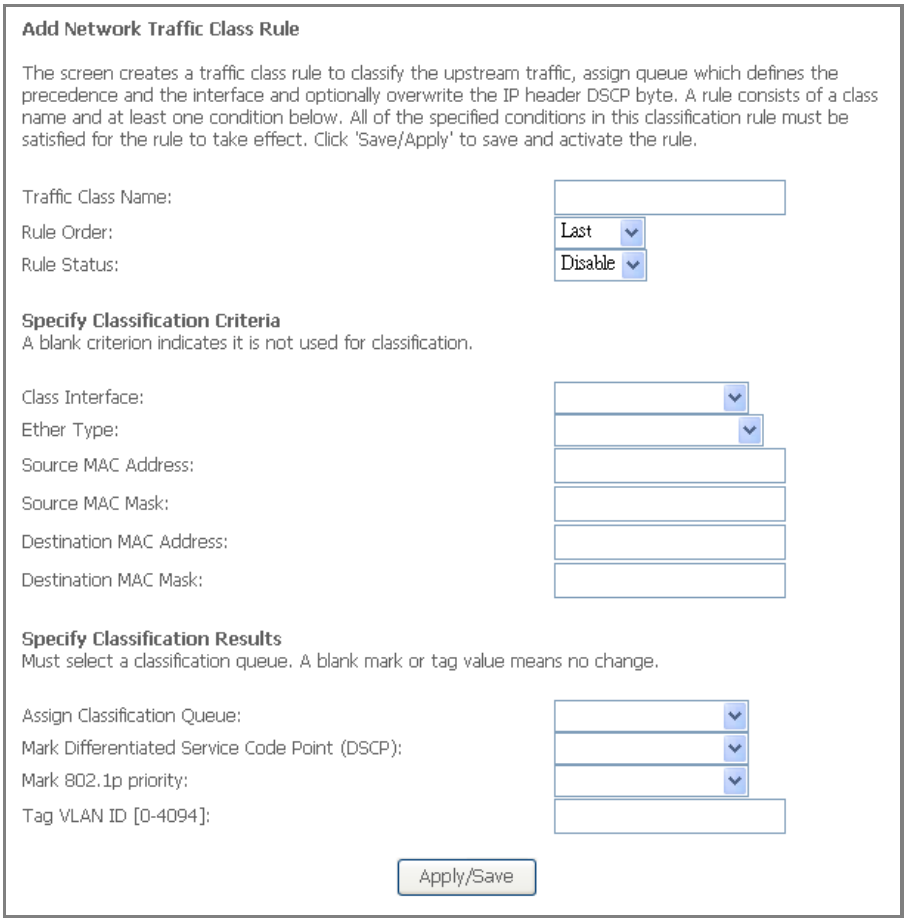
Precedence	Meaning	Precedence	Meaning
0	Routine	4	Flash Override
1	Priority	5	Critical
2	Immediate	6	Internetwork Control
3	Flash	7	Network Control

5.7.2 QoS Classification

This page allows you to crate a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.



Click **Add** to configure QoS classification. Enter the settings and then click **Apply/Save**.

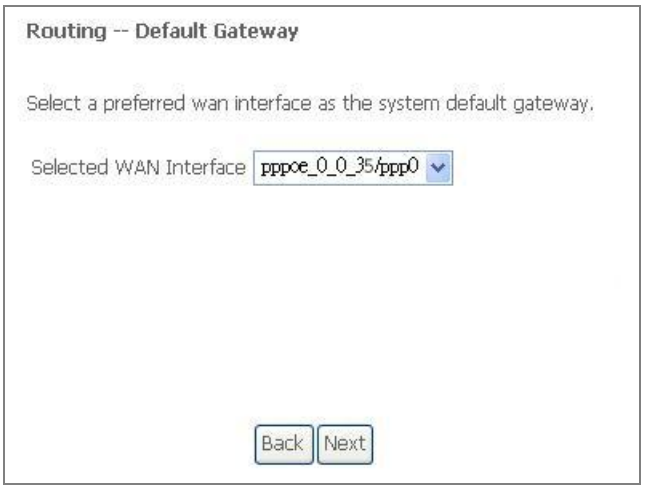


Field	Description
Traffic Class Name	Enter a name for this traffic class.
Rule Order	Select a rule order for this traffic class.
Rule Status	Select to enable or disable this traffic class.
Class Interface	Select an interface for this traffic class to apply.
Ether Type	Select the Ether type from the drop-down list.
Source MAC Address/Mask	Enter the MAC address and the mask of the computer where packets are coming from.
Destination MAC Address/Mask	Enter the MAC address and the mask of the computer where the packets will be sent to.
Assign Classification Queue	Select the classification queue for the traffic class.
Mark DSCP	Select the DSCP to mark. Different markers representing different grades of service placed on various packet streams to be recognized by the router for route purposes.
Mark 802.1p Priority	If 802.1q was enabled on WAN, then select a value between 0-7.
Tag VLAN ID	Enter a VLAN ID for the packet to tag.

5.8 Routing

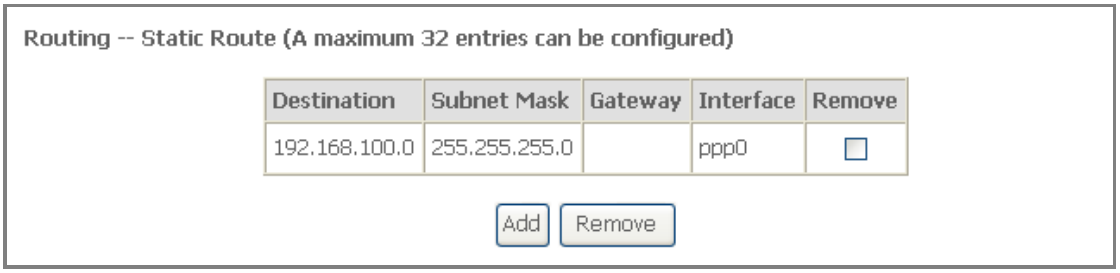
5.8.1 Default Gateway

This page allows you to select a preferred WAN interface to be the system's default gateway.



5.8.2 Static Route

This page allows you to add the routing table. A maximum of 32 entries can be configured.



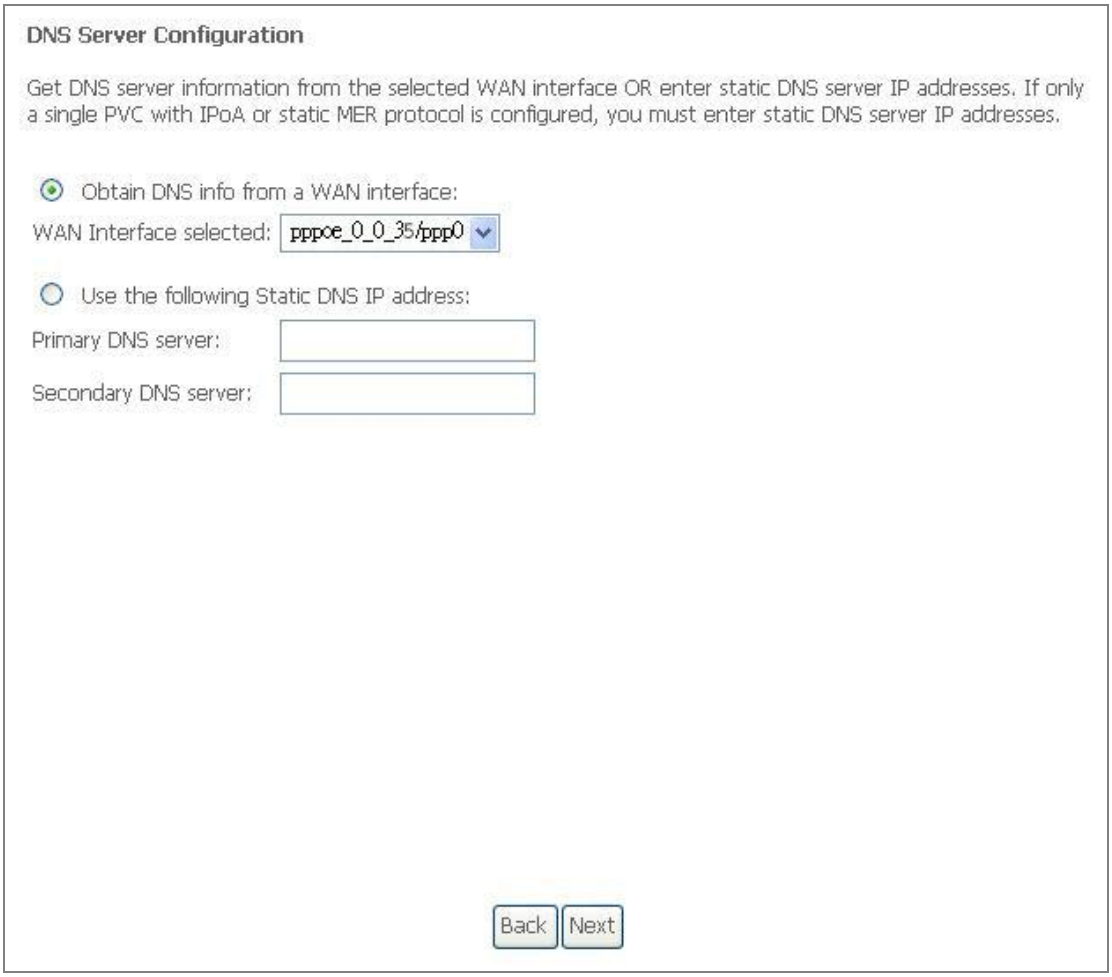
Click **Add** to configure the routing table. Enter the routing information and then click **Save/Apply**.

Field	Description
Destination Network Address	Enter the destination address of the LAN IP.
Subnet Mask	Enter the subnet mask of the LAN IP.
Use Interface	Check and select a WAN interface for static route.
Use Gateway IP Address	Check and enter the gateway address of the remote router.

5.9 DNS

5.9.1 DNS Server

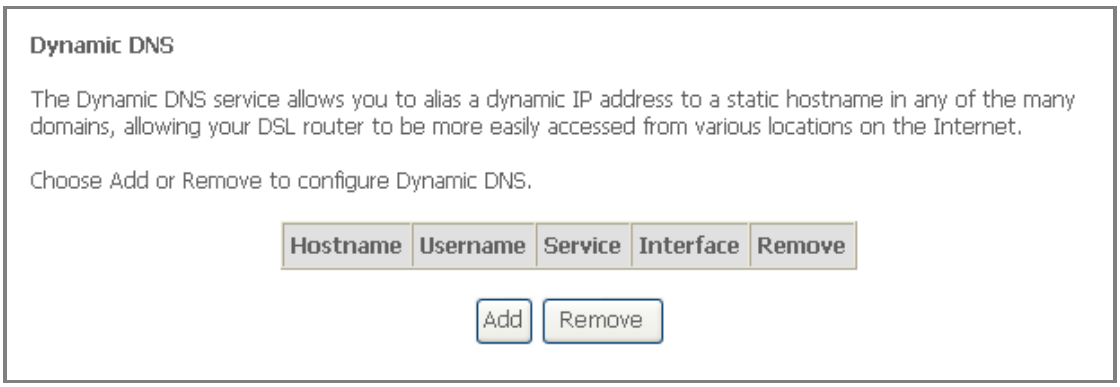
This page allows you to enable automatic DNS from the ISP or specify their own DNS server address manually.



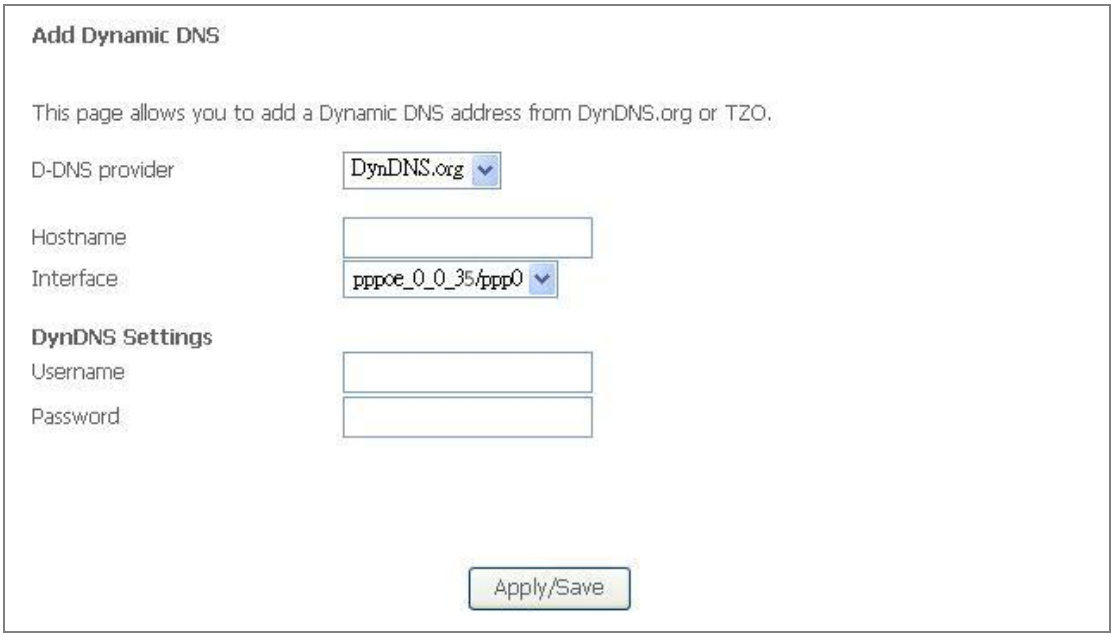
Field	Description
Obtain DNS Info from a WAN	Select the WAN interface to obtain the DSN info.
Use the Following Static DNS IP Address	Select to configure the static DNS IP address manually.
Primary DNS Sever	Enter the IP address of primary DNS server.
Secondary DNS Sever	(Optional) Enter the IP address of secondary DNS server.

5.9.2 Dynamic DNS (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing the INNOBAND DSL to be easily accessed from various locations on the Internet.



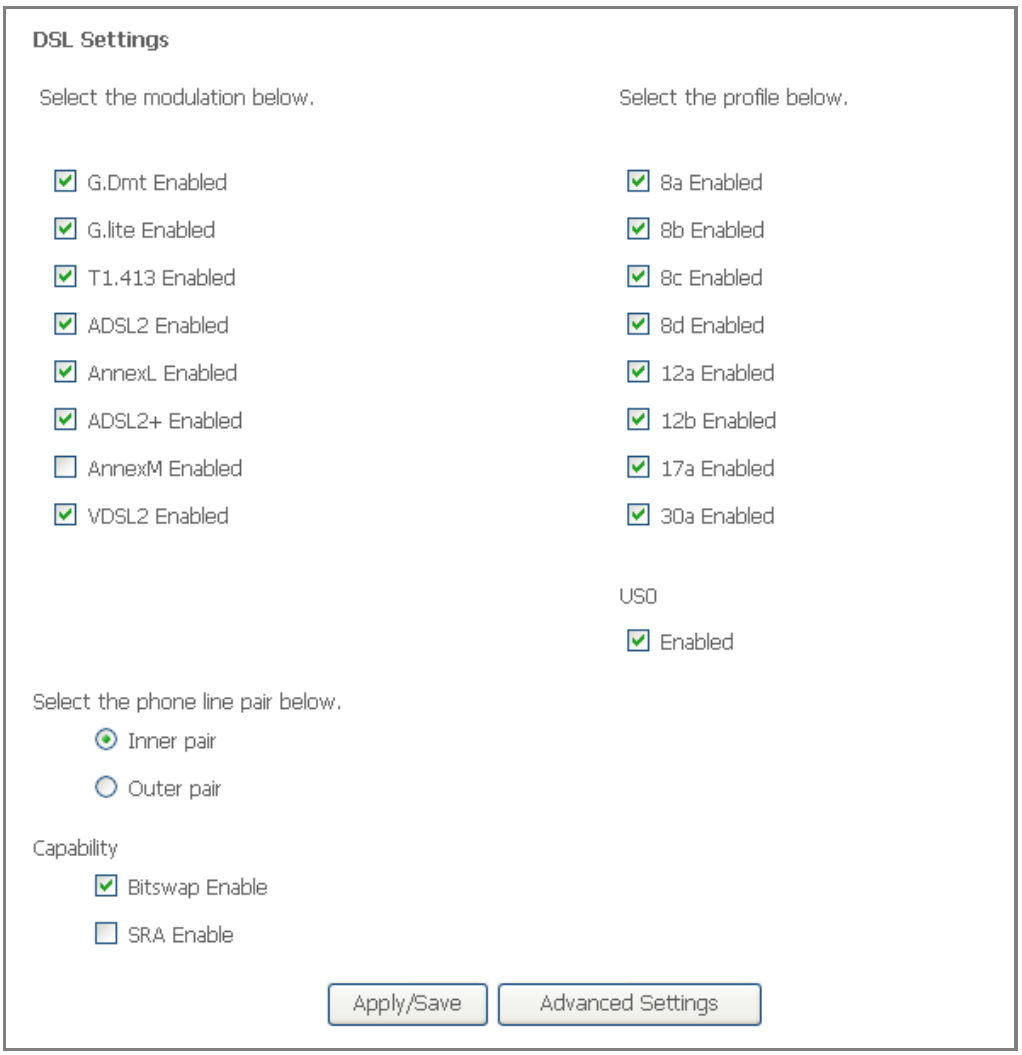
Click **Add** to configure the DDNS. This page allows you to set up DDNS address from DynDNS.org. You must register with the service provider first and obtain the necessary information. Enter the DDNS information and then click **Save/Apply**.



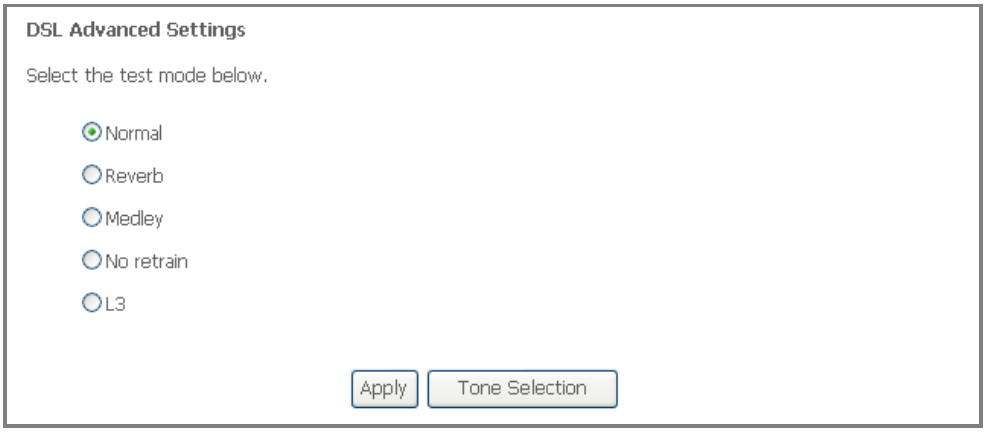
Field	Description
D-DNS Provider	INNOBAND DSL is pre-configured with the DynDNS.org as DDNS provider.
Hostname	Enter the host name.
Interface	Select a WAN interface to apply DDNS service.
DynDNS Username / Password	Enter username and password of your account on DysDNS.org.

5.10 DSL

This page allows you to select the modulation, phone line type and capability specified by your ISP. The default configuration in this page can work with most VDSL implementations. DO NOT change any setting unless you are instructed to do so. Then click **Save/Apply**.



If you want to configure more advanced setting, click **Advanced Settings**. Select the test mode for DSL line.



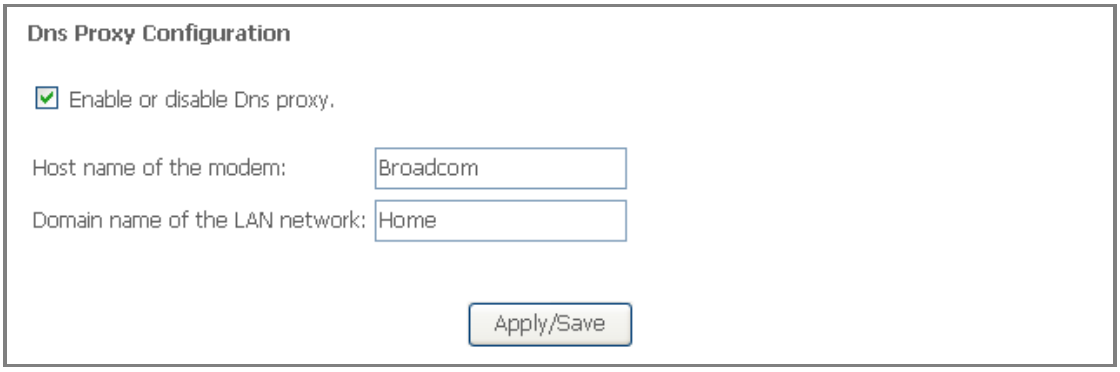
5.11 UPnP

This page allows you to enable the UPnP function. The UPnP function allows devices to connect seamlessly and to simplify the implementation of networks such as data sharing, communications and entertainment.

The UPnP feature requires one active WAN interface. You must create one WAN connection before you can enable this function. In addition, the client connecting to the INNOBAND DSL should also support this feature.

5.12 DNS Proxy

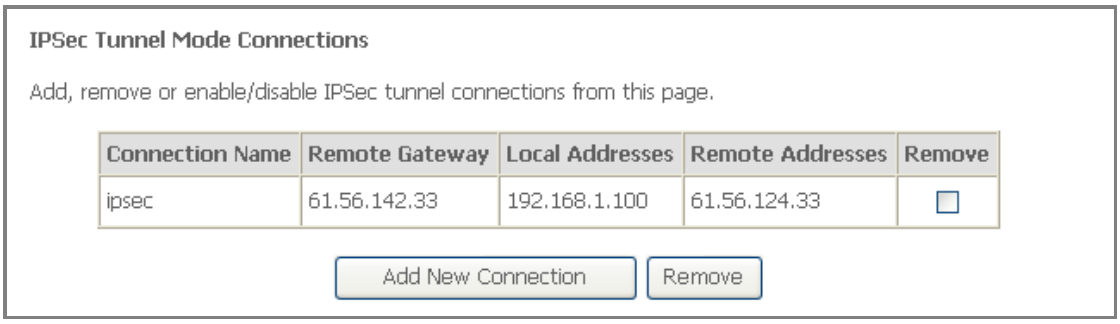
The INNOBAND DSL can acts as a DNS proxy when you enable DNS proxy feature.



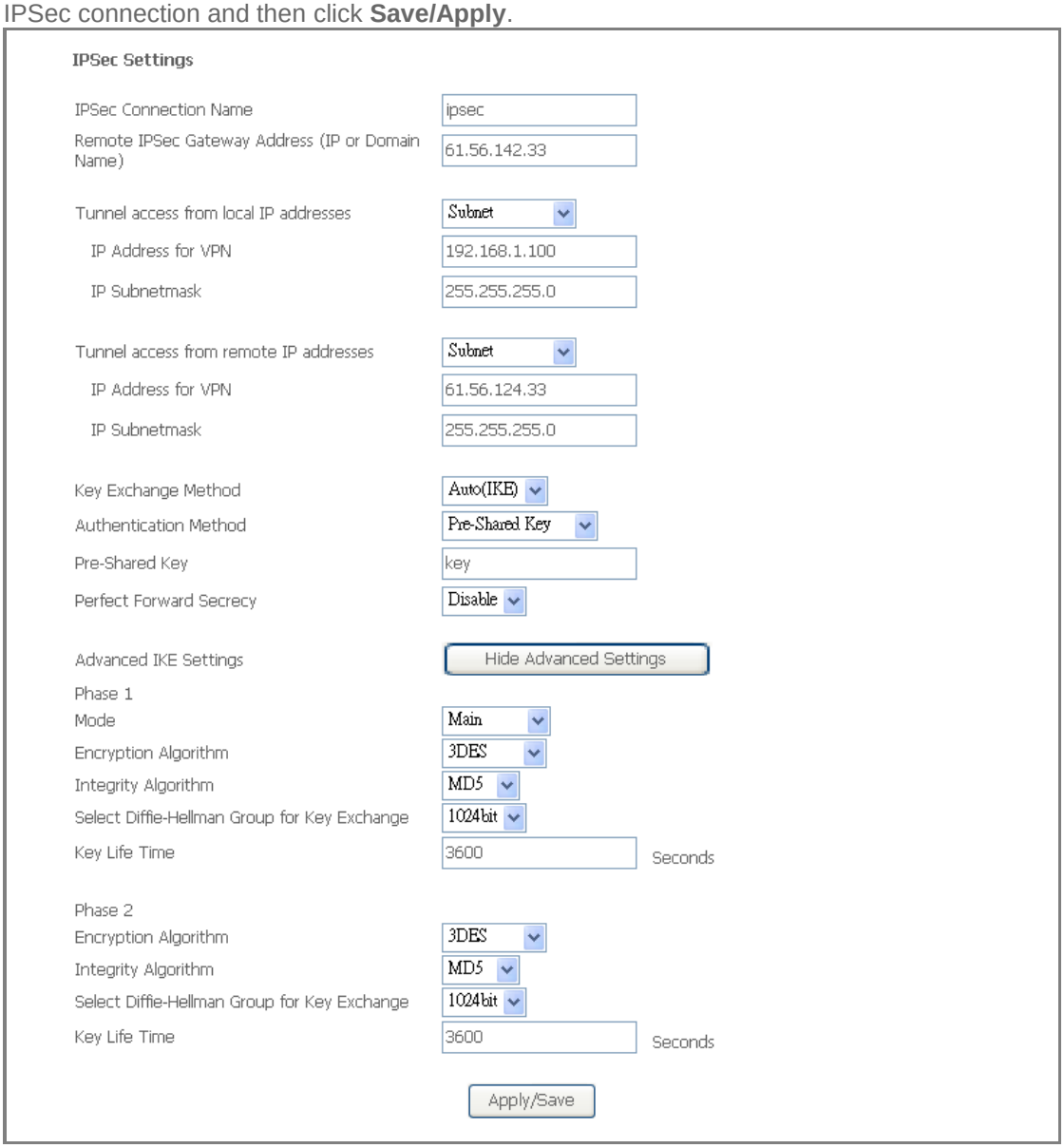
Field	Description
Enable DNS Proxy	Check to enable DNS proxy feature.
Host Name of the modem	Enter a host name for the INNOBAND DSL.
Domain name of the LAN Network	Enter a name for this LAN network.

5.13 IP Sec

This page shows the IPSec Tunnel connection.



Click **Add New Connection** to add a new IPSec Tunnel connection. Enter the setting for IPSec connection and then click **Save/Apply**.



Field	Description
IPSec Connection Name	Enter a name for this IPSec connection.
Remote IPSec Gateway Address	Enter the IP address or domain name of the remote IPSec gateway.
Tunnel Access From Remote / Local IP Addresses	Select the range of local / remote IP addresses from the drop-down list.
IP Address for VPN	Specify the remote / local IP address for VPN.
IP Subnet Mask	Specify the subnet mask for the remote / local IP address.
Key Exchange Method	Select the key exchange method to be auto or manual.
Authentication Method	Select the authentication method to be Pre-Share Key or Certificate X.509.
Pre-Shared Key	Specify the Key if you select the authentication method as Pre-Shared Key.
Certificate	Select the certificate from drop-down list if you select the authentication method as Certificate X.509.
Perfect Forward Secrecy	Select to enable or disable Perfect Forward Secrecy (PFS) feature.
Encryption Algorithm	Select the encryption algorithm to be DES, 3DES or AES (aec-cbc).
Encryption Key	Enter the encryption key to be 3DES or AES (Advanced Encryption Standard).
Authentication Algorithm	Select the authentication algorithm from drop-down list.
Authentication Key	Enter the authentication key to be MD5 or SHA1.
SPI	Enter the SPI (Security Parameter Index) which is an identification tag added to the header tunneling the IP traffic.

There are two phases of IPSec:
Phase 1: Start to negotiate IKE parameters including encryption, integrity (hash), Diffie-Hellman parameter values and lifetime to protect the following IKE exchange. The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority to match with its policies. This sets up a secure tunnel for IKE Phase 2.

Phase 2: Start to negotiate IPSec security for the following IKE exchange and mutual examination of the secure tunnel establishment.


Note

It is critical that the exact same Phase 1 and Phase 2 proposals be entered at the remote client.

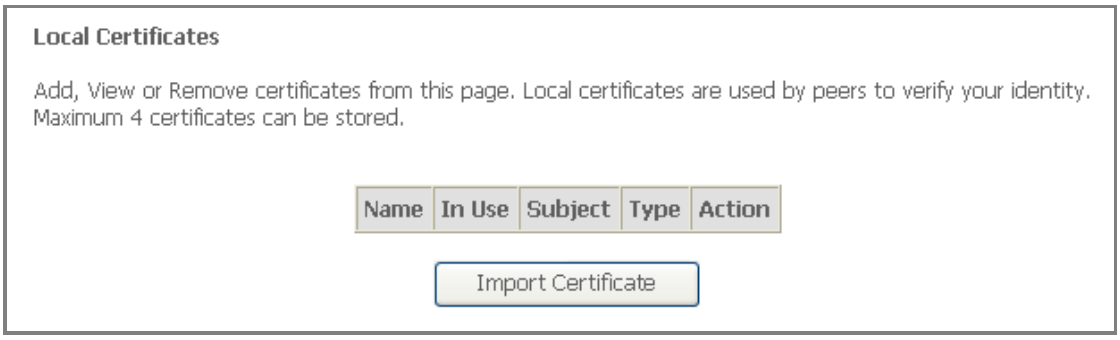
Field	Description
Advanced IKE Settings	This button is available when you select the **Key Exchange Method** as Auto mode.
Mode	Select the mode to be Main or Aggressive.
Encryption Algorithm	Select the encryption algorithm to be DES, 3DES, AES-128, AES-196 or AES-256.
Integrity Algorithm	Select the integrity algorithm to be MD5 or SHA1.
Select Diffie-Hellman Group for Key Exchange	Select the Diffie-Hellman group to be 768, 1024, 1536, 2048, 3072, 4096, 6144 or 8192-bit for key exchange.
Key Life Time	Configure the life time for Key (in second).

5.14 Certificate

This section allows you to create certificates.

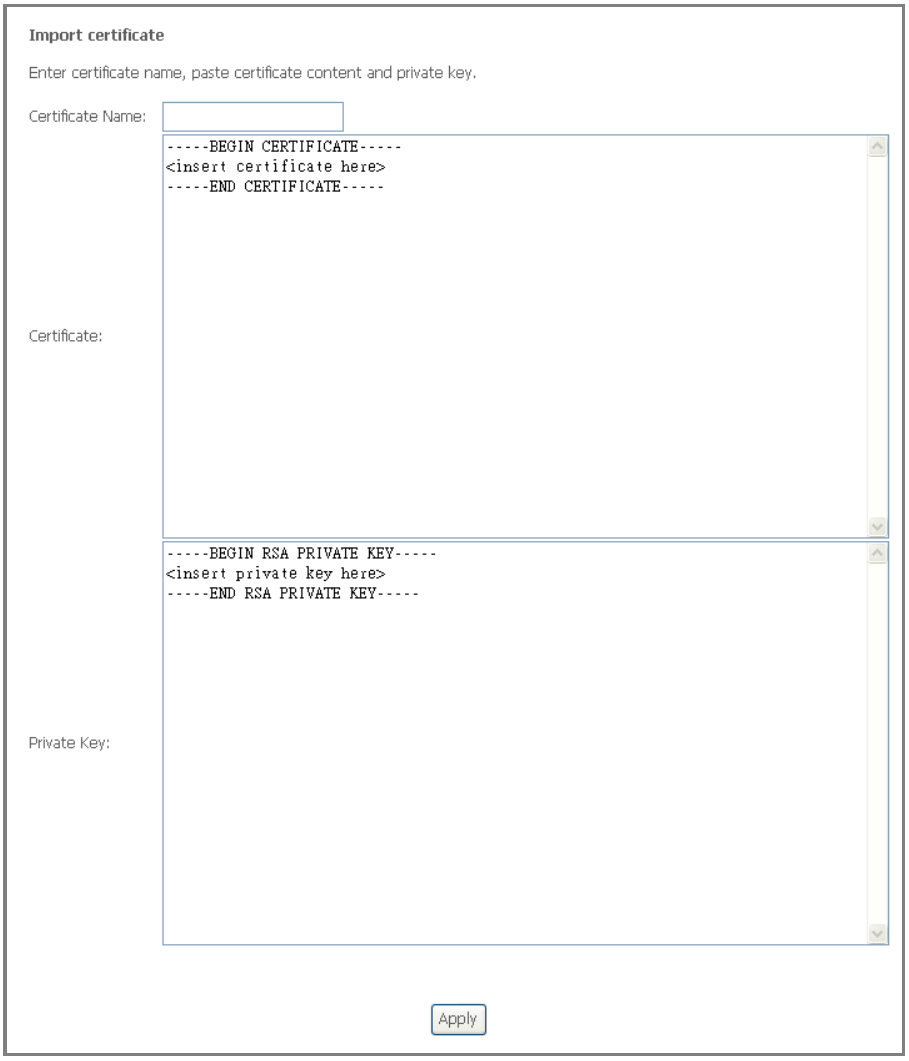
5.14.1 Local

This page allows you to crate local certificate. Local certificates are used by peers to verify your identity. You can either create certificate request or import the certificate to add local certificates. Maximum 4 certificates can be stored.



Click **Import Certificate** to import the certificate.

Enter a certificate name, paste the certificate content and private key to create the certificate. Then click **Apply**.



5.14.2 Trusted CA

If an entity wants to utilize digital certificates, this entity should retrieve certificates of trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers. Maximum 4 certificates can be stored.

Click **Import Certificate** to import the certificate. Enter a certificate name and paste the certificate content to create the certificate. Then click **Apply**.

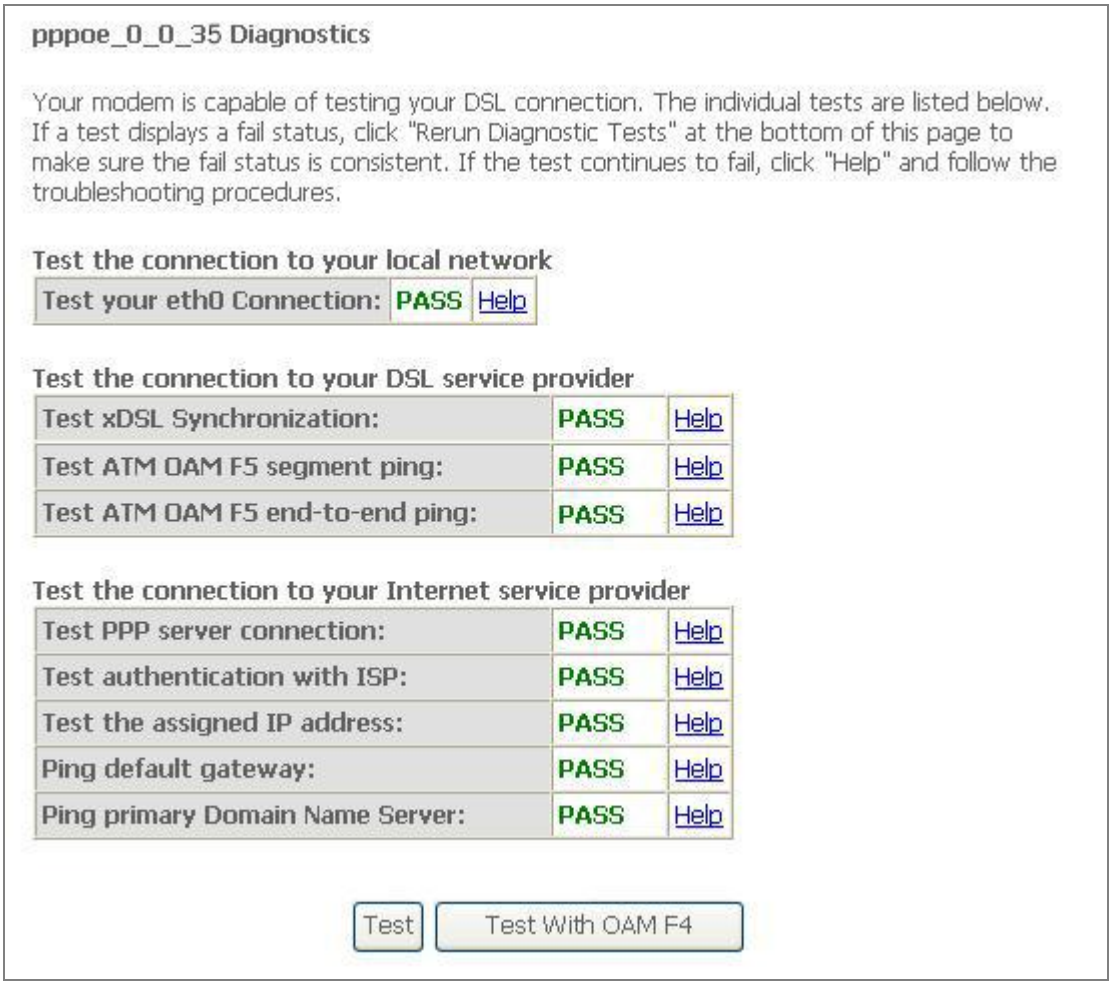

Import CA certificate
Enter certificate name and paste certificate content.
Certificate Name:
Certificate:
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
Apply

6. Diagnostics

This page shows the VDSL diagnostic information. Usually, you do not have to view this data, but you may find it useful when working with your ISP to diagnose network and Internet data transmission problems.

6.1 Diagnostics

If a test displays a fail status, click "Test" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.



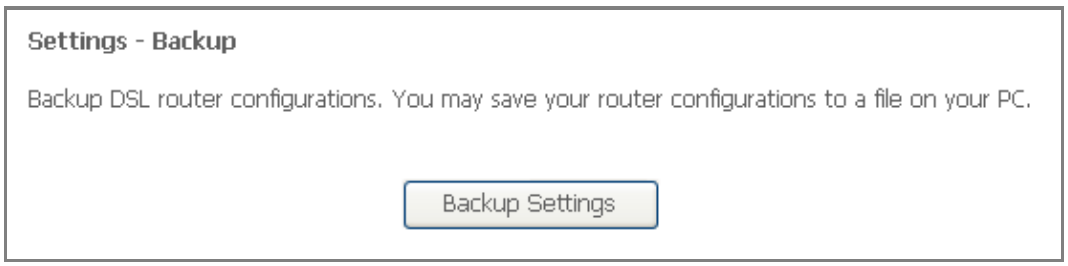
7. Management

This section allows you to maintain the system, including backing up the configurations, viewing system log, maintaining access control and updating software.

7.1 Settings

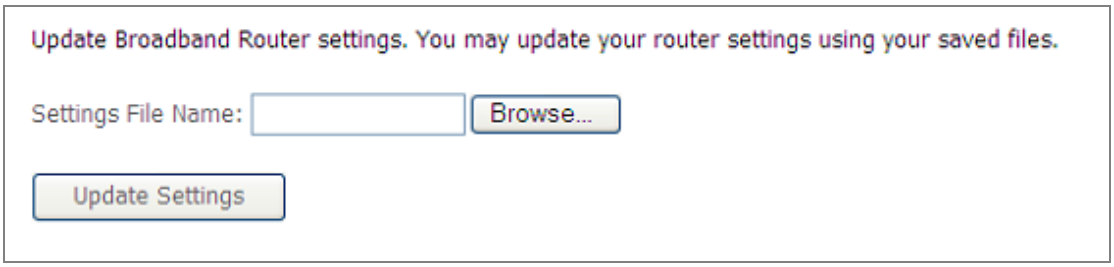
7.1.1 Backup

This page allows you to backup (copy) current settings to a file on your PC.



7.1.2 Update

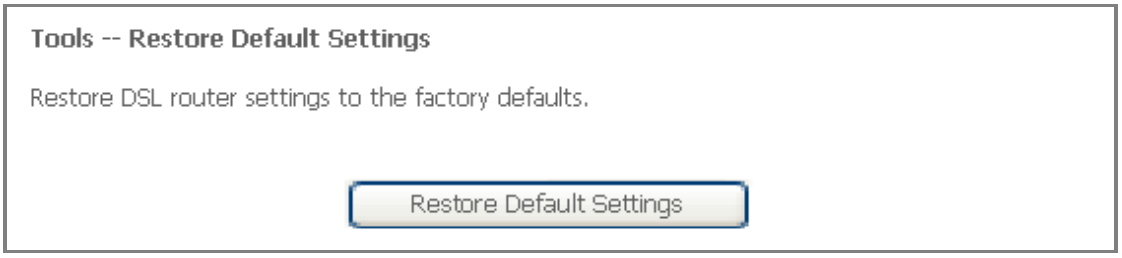
This page allows you to restore the settings from a previously saved file.



To restore a previously saved configuration file onto the INNOBAND DSL, click **Browse** to find the file on your PC and click **Update Settings**. The INNOBAND DSL restores settings and reboots to activate the restored settings.

7.1.3 Restore Default

This page allows you to reset the configuration to default settings. It deletes all current settings and resets the INNOBAND DSL to factory default settings.

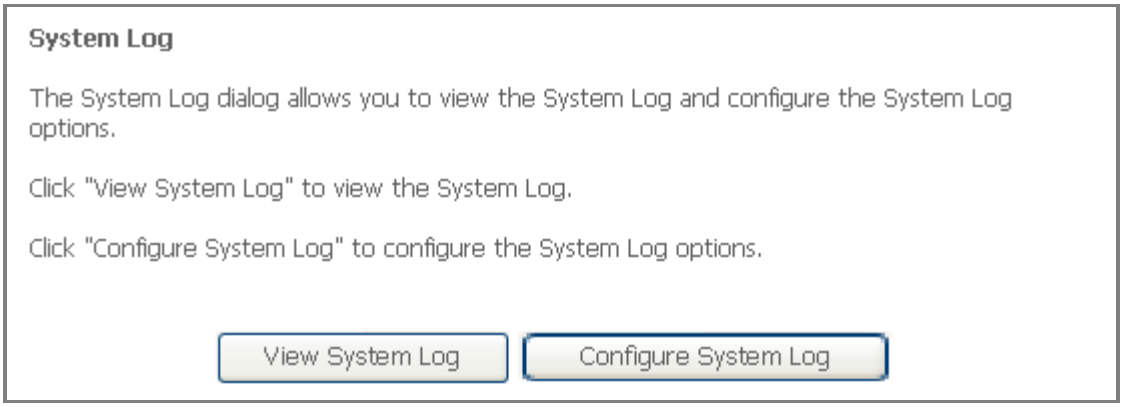


Click **Restore Default Settings** and click **OK** when the pop-up window appears confirming that you want to restore factory default settings to your INNOBAND DSL. The INNOBAND DSL restores the default settings and reboots.

IMPORTANT!	*DO NOT power off the INNOBAND DSL or press the reset button while this process is in progress.*

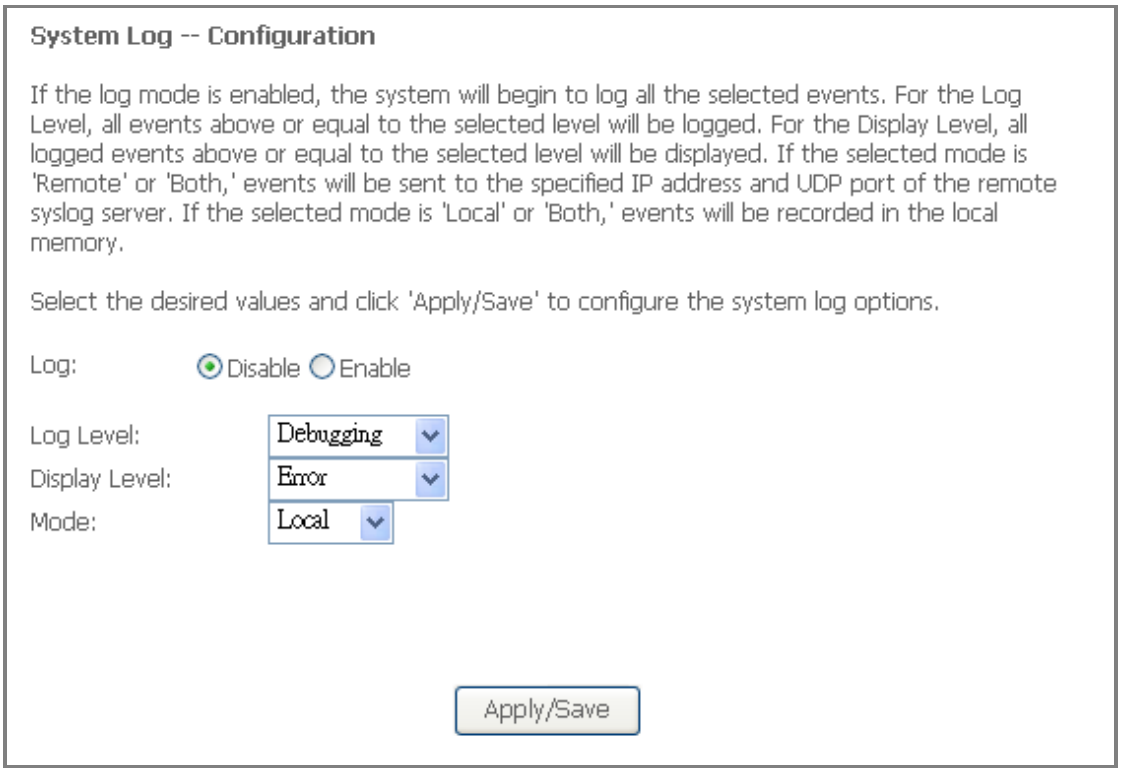
7.2 System Log

This dialog allows you to view system log and configure system log options. To view the System Log, click **View System Log**. To configure System Log, click **Configure System Log**.



7.2.1 Configure System Log

This page allows you to configure the system log level and display level. You must enable the System Log function so that the INNOBAND DSL can log the selected events.



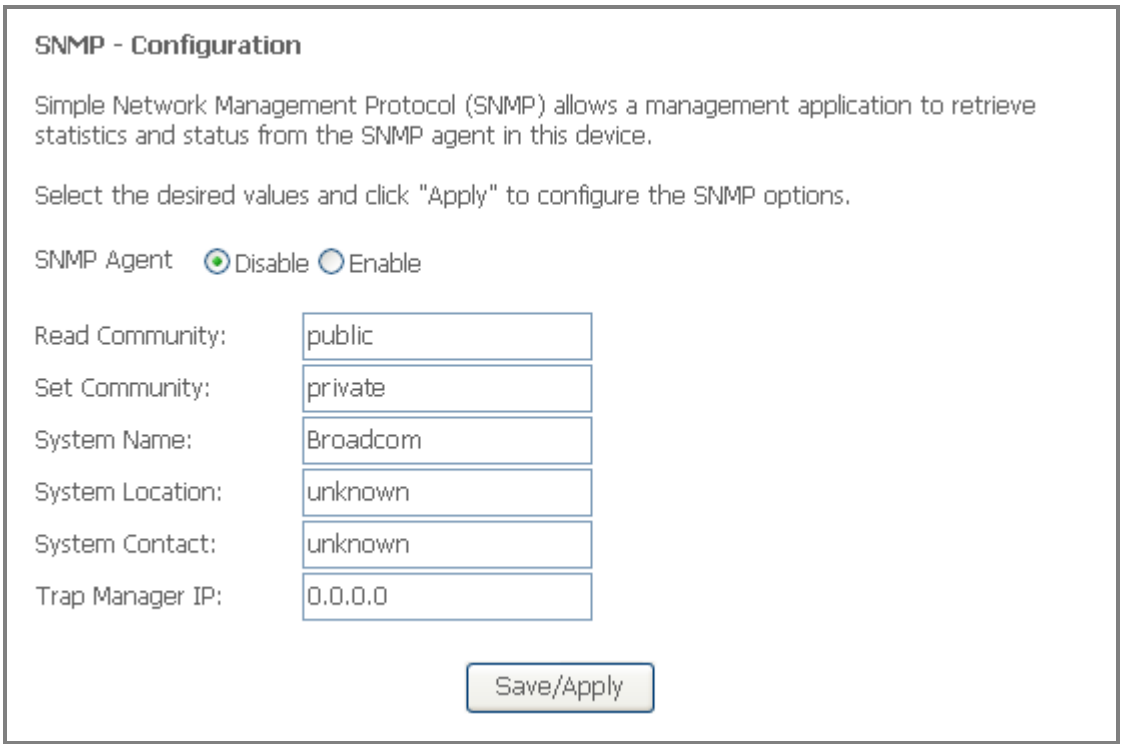
Field	Description
Log Level	Select level of application events to log.
Display Level	Select level of application events to display.
Mode	Select to record the events in the local memory, sent them to a remote system log server or both.
Server IP Address	Enter the IP Address of remote system log server.
Server UDP Port	Enter the UDP port of the remote system log server.

7.2.2 View System Log

This page shows the events of INNOBAND DSL. If the system log feature is enabled, the system will log selected events. All events above or equal to the selected log level will be logged and displayed.

7.3 SNMP Agent

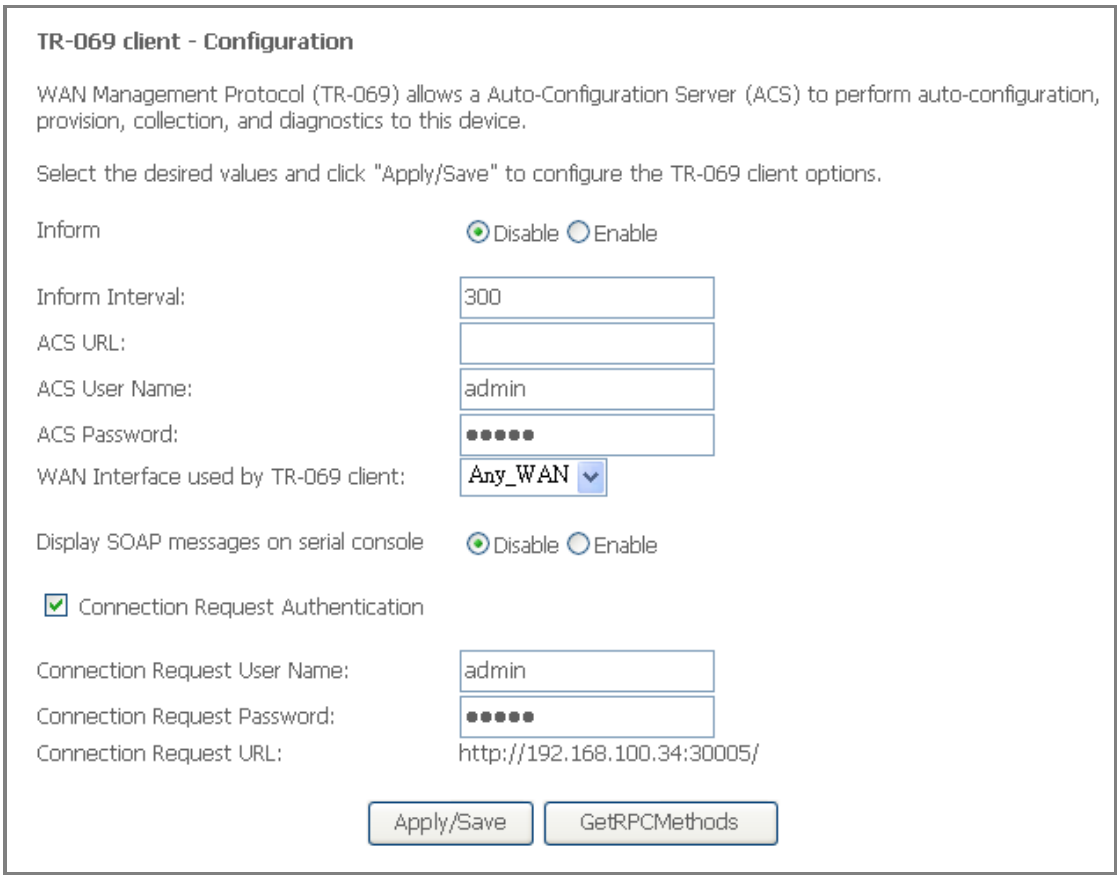
The SNMP (Simple Network Management Protocol) allows the management application to retrieve statistics and status from the SNMP agent in this device.



Field	Description
Read Community	Enter the password (character string) to specify the read privilege between the SNMP agent and manager.
Set Community	Enter the password (character string) to specify the write privilege between the SNMP agent and manager.
System Name	Enter the System name of the SNMP agent
System Location	Enter the System location of the SNMP agent
System Contact	Enter the System contact of the SNMP agent.
Trap Manager IP	Enter the IP address of the Trap Manager.

7.4 TR-069 Client

The INNOBAND DSL includes a TR-069 client which is a WAN management protocol. All the values are already filled in.

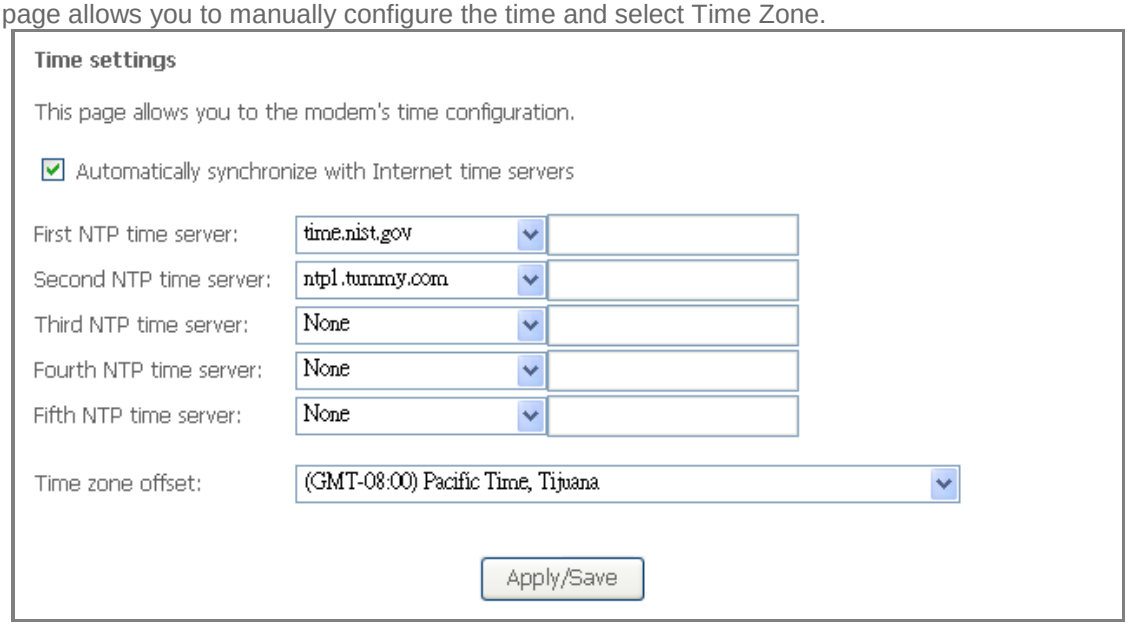


Field	Description
Inform	Enable or disable the INNOBAND DSL to connect to the ACS periodically.
Inform Interval	Enter the amount of time (in second) between a successful connection with an ACS server and a new attempt to connect to an ACS server. This field is enabled only when the Inform **Enabled** is selected.
ACS URL	Enter the URL of the Auto Configuration Server (ACS) provided by the ISP.
ACS User Name	Enter the user name for the ACS to authenticate.
ACS Password	Enter the password for the ACS to authenticate.
WAN Interface Used by TR-069 Client	Select the WAN interface from the drop-down for TR-069 client to use.
Display SOAP messages on serial console	Enable or disable whether display SOAP messages on serial console or not.
Connection Request Authentication	Check to enable connection request authentication.
Connection Request User Name	Enter the username used to authenticate an ACS making a connection request to the INNOBAND DSL.

Connection Request Password	Enter the password used to authenticate an ACS making a connection request to the INNOBAND DSL.
Connection Request URL	This is the URL of connection request.
GetRPCMethods	Click this button to force the INNOBAND DSL to immediately establish a connection to the ACS.

7.5 Internet Time

This page allows you to manually configure the time and select Time Zone.



Field	Description
Automatically synchronize with Internet time server	Check to enable the INNOBAND DSL to synchronize with Internet time server to update the system clock.
First/ Second/ Third/ Fourth/ Fifth NTP time server	Select at least one Internet time server from drop-down list or specify its IP address manually.
Time Zone Offset	Select The time zone in which the INNOBAND DSL resides.

7.6 Access Control

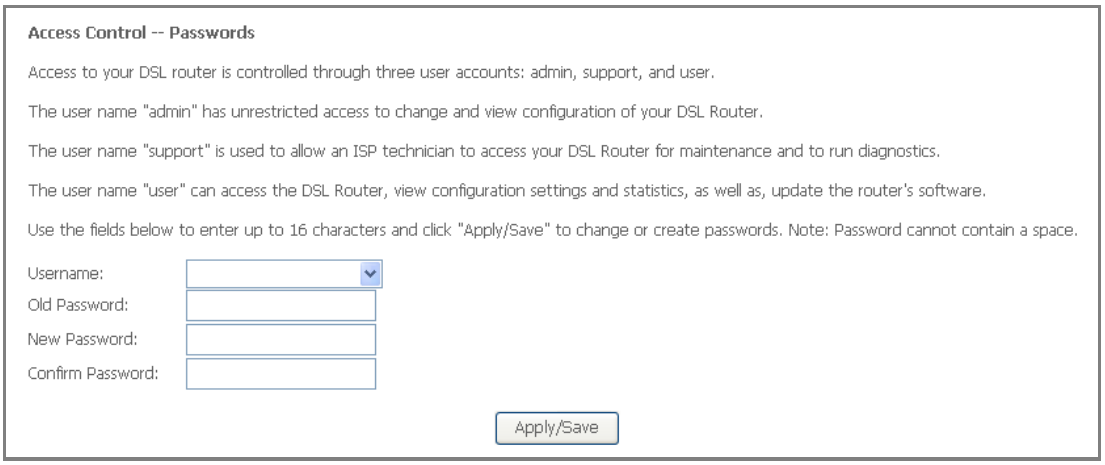
7.6.1 Passwords

This page allows you to change the password for all users account. Access to your INNOBAND DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of the INNOBAND DSL

The user name "support" is used to allow an ISP technician to access your INNOBAND DSL for maintenance and to run diagnostics.

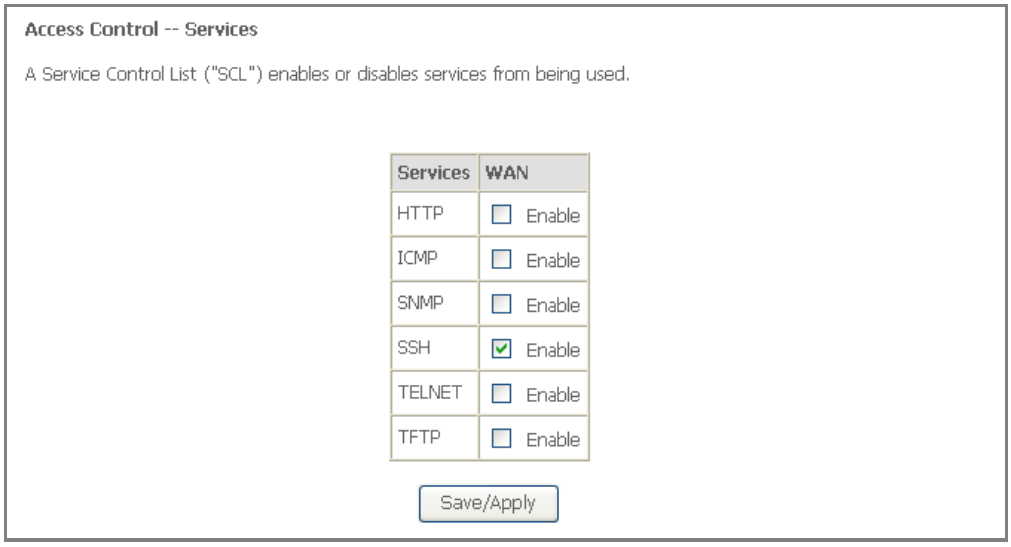
The user name "user" can access the INNOBAND DSL, view configuration settings and statistics, as well as, update the router's software.



Field	Description
Username	Enter the pre-defined username from drop-down list.
Old Password	Enter the old password of this account.
New Password	Enter the new password for this account.
Confirmed Password	Enter the new password for this account again to confirm the password.

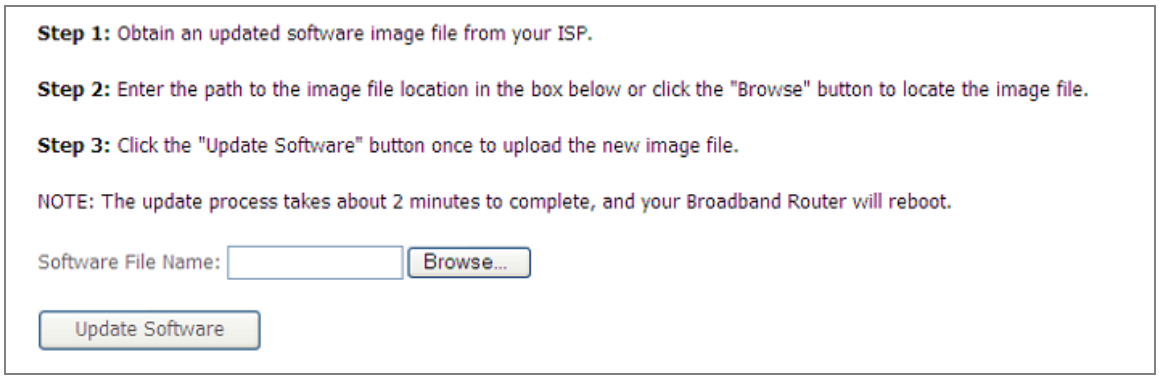
7.6.2 Services

This page allows you to enable or disable the services from being used for WAN.



7.7 Update Software

The system software used by this INNOBAND DSL is called “firmware”. This page allows you to upgrade the firmware to a newer version.



This page allows you to update the software (firmware) of INNOBAND DSL to a newer version. If your ISP releases new software for INNOBAND DSL, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Click Browse to locate the image file.
3. Click Update Software to upload the new image file.

Note

The update process takes about 2 minutes to complete, and your DSL Router will reboot.

IMPORTANT!	*DO NOT power off the INNOBAND DSL or press the reset button while this process is in progress.*

7.8 Reboot

This page allows you to reboot the INNOBAND DSL.

IMPORTANT!	*DO NOT power off the INNOBAND DSL or press the reset button while this process is in progress.*

8. Troubleshooting

If the suggested solutions in this section do not resolve your issue, contact your system administrator or Internet service provider.

8.1 Problems with LAN access

PCs on the LAN cannot get IP addresses from the Router

- The chances are that the interface used as DHCP server is modified and the client PCs do not renew IP addresses.
- If your DHCP server is enabled on Private IP Address previously and you modify the interface to Public IP Address, the client PCs should renew IP addresses.
- The PC on the LAN cannot access the Web page of the Router.
  Check that your PC is on the same subnet with the Router.
- The virtual server can't be access after setting virtual server.
  Check the filter rule of the port that virtual server service setting for example, the virtual server service set FTP 21 you need update the filter rule of the ftp 21 **Direction** setting**:** Choose filter the packets that incoming action (In Bound) are **Allow** on the interface.

8.2 Problems with WAN access

You cannot access the Internet.

- Check the physical connection between the Router and the LAN.If the LAN LED on the front panel is off or keeps blinking, there may be problem on the cable connecting to the Router. At the DOS prompt, ping the IP address of the Router, e.g, ping 192.168.1.1. If the following response occurs:
  Relay from 192.168.1.1 bytes=32 time=100ms TTL=253
  Then the connection between the Router and the network is OK.
  If you get a failed ping with the response of: Request time out
  Then the connection is fail. Check the cable between the Router and the network.
- Check the DNS setting of the Router.
  At the DOS prompt, ping the IP address of the DNS provided by your ISP. For example, if your DNS IP is 168.95.1.1, then ping 168.95.1.1. If the following response occurs: Relay from 168.95.1.1 bytes=32 time=100ms TTL=253
  Then the connection to the DNS is OK.
  If you get a failed ping with the response of:
  Request time out
  Then the DNS is not reachable. Check your DNS setting on the Router.

8.3 Glossary

ARP - Address Resolution Protocol

ARP is a TCP/IP protocol for mapping an IP address to a physical machine address that is recognized in the local network, such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
Inverse ARP (In-ARP), on the other hand, is used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

BPS - Bits Per Second

The rate of data flow.

Broadband

High-capacity high-speed, transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.

DHCP (Dynamic Host Configuration Protocol)

When operates as a DHCP server, the Router assign IP addresses to the client PCs on the LAN. The client PCs "leases" these Private IP addresses for a user-defined amount of time. After the lease time expires, the private IP address is made available for assigning to other network devices.
The DHCP IP address can be a single, fixed public IP address, an ISP assigned public IP address, or a private IP address.
If you enable DHCP server on a private IP address, a public IP address will have to be assigned to the NAT IP address, and NAT has to be enabled so that the DHCP IP address can be translated into a public IP address. By this, the client PCs are able to access the Internet.

DHCP Server

A server or service with a server that assigns IP addresses.

DNS - Domain Name System

A system for converting host names and domain names into
IP addresses on the Internet or on local networks that use the TCP/IP protocol.

Firewall

A hardware or software boundary that protects a network or single computer from unwanted outside traffic.

Firmware

A computer program embedded in an electronic device Firmware usually contains operating code for the device.

FTP - File Transfer Protocol

A network protocol for exchanging files over a TCP network. Gateway — A network point that acts as an entrance to another network that uses a different protocol.

Host Name

The unique name by which a network-attached device is known on a network.

HTTP - Hypertext Transfer Protocol
An application-level protocol for accessing the World Wide Web over the Internet.

IMAP - Internet Message Access Protocol
An Internet standard protocol for email retrieval.

IP - Internet Protocol
The mechanism by which packets are routed between computers on a network.

IP Type
The type of service provided over a network.

IP address - Internet Protocol address
The address of a device attached to an IP network (TCP/IP network)

ISP - Internet Service Provider
Also referred to as the service carrier, an ISP provides Internet connection service.
Kbps - Kilobits per second
The rate of data flow.

LAN - Local Area Network & WAN - Wide Area Network
A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN, on the other hand, is an outside connection to another network or the Internet.
The Ethernet side of a Router is called the LAN port. It is a twisted-pair Ethernet 10Base-T interface. A hub can be connected to the LAN port. More than one computer, such as server or printer, can be connected through this hub to the Router and composes a LAN.

MAC Address - Media Access Control
A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers.

Mbps - Megabits per second
The rate of data flow.

NAT - Network Address Translation - IP Address
NAT is an Internet standard that translates a private IP within one network to a public IP address, either a static or dynamic one. NAT provides a type of firewall by hiding internal IP addresses. It also enables a company to use more internal IP addresses.
If the IP addresses given by your ISP are not enough for each PC on the LAN and the Router, you need to use NAT. With NAT, you make up a private IP network for the LAN and assign an IP address from that network to each PC. One of some public addresses is configured and mapped to a private workstation address when accesses are made through the gateway to a public network.
For example, the Router is assigned with the public IP address of 168.111.2.1. With NAT enabled, it creates a Virtual LAN. Each PC on the Virtual LAN is assigned with a private IP address with default value of 192.168.1.2 to 192.168.2.254. These PCs are not accessible by the outside world but they can communicate with the outside world through the public IP 168.111.2.1.

Network Mask
A number that allows IP networks to be subdivided for security and performance.

Network Provider
The vendor who provides your access to the Internet. Known by different names in different regions, some examples are: wireless provider, network operator, and service provider.

Network Technology
The technology on which a particular network provider's system is built; such as, xDSL, PON, GPON, GSM, HSPA, CDMA, EDGE, and EVDO.

NNTP - Network News Transfer Protocol
An Internet application protocol for reading and posting Usenet (newsgroup) articles.

POP - Post Office Protocol
An Internet protocol for retrieving email from a remote server over a TCP/IP connection.
Port. A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

Port Forwarding
A process that allows remote devices to connect to a specific computer within a private LAN.

Port Number
A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.

Private IP Address
Private IP addresses are also LAN IP addresses, but are considered "illegal" IP addresses to the Internet. They are private to an enterprise while still permitting full network layer connectivity between all hosts inside an enterprise as well as all public hosts of different enterprises.
The Router uses private IP addresses by assigning them to the LAN that cannot be directly accessed by the Internet or remote server. To access the Internet, private network should have an agent to translate the private IP address to public IP address.

Protocol
A standard that enables connection, communication, and data transfer between computing endpoints.

PPP - Point to Point Protocol
A method of connecting a computer to the Internet.

Protocol
A standard that enables connection, communication, and data transfer between computing endpoints.

Proxy
A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.

Public IP Address
Public IP addresses are LAN IP addresses that can be considered "legal" for the Internet, because they can be recognized and accessed by any device on the other side of the DSL connection. In most cases they are allocated by your ISP.

If you are given a range of fixed IP addresses, then one can be assigned to the router and the others to network devices on the LAN, such as computer workstations, ftp servers, and web servers.

PVC - Permanent Virtual Circuit
A PVC is a logical point-to-point circuit between customer sites. PVC's are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is pre-programmed by the carrier as a path through the network. It does not need to be set up or turned down for each session.

RIP - Routing Information Protocol
RIP is a routing protocol that uses the distance-vector routing algorithms to calculate least-hops routes to a destination. It is used on the Internet and is common in the NetWare environment. It exchanges routing information with other routers. It includes V1, V2 and V1&V2, which controls the sending and receiving of RIP packets over Ethernet.

Router
A device that directs traffic from one network to another.

RTP - Real-time Transport Protocol
A packet format for streaming multimedia over the Internet.

SMTP - Simple Mail Transfer Protocol
An Internet standard for email transmission across IP networks.

TCP - Transmission Control Protocol
A core protocol for transmitting and receiving information over the Internet.

TCP/IP - Transmission Control Protocol / Internet Protocol
A communications protocol developed under contract from the U.S. Department of Defence to internetwork dissimilar systems.

Telnet - Telecommunication Network
A network protocol used on the Internet or on local area networks.

TFTP - Trivial File Transfer Protocol
A file transfer protocol with a subset of FTP functionality.

UDP - User Datagram Protocol
UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.

VPI - Virtual Path Identifier & VCI - Virtual Channel Identifier
A VPI is a 8-bit field while VCI is a 16-bit field in the ATM cell header. A VPI identifies a link formed by a virtual path and a VCI identifies a channel within a virtual path. In this way, the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cell is following, unassigned cells, physical layer OAM cells, meta-signalling channel or a generic broadcast signalling channel. Your ISP should supply you with the values.

Virtual Server

You can designate virtual servers, e.g., a FTP, web, telnet or mail server, on your local network and make them accessible to the outside world. A virtual server means that it is not a dedicated server -- that is, the entire computer is not dedicated to running on the public network but in the private network.

VNC - Virtual Network Computing
A graphical desktop sharing system that uses the RFB protocol to remotely control another computer.

VPN Pass through
A feature that allows a client to connect to a VPN server.

WAN - Wide Area Network
A public network that extends beyond architectural, geographical, or political boundaries (unlike a LAN, which is usually a private network located within a room, building, or other limited area).

9. Safety Notes

9.1.1 For Installation

- Use only the type of power source indicated on the marking labels.
- Use only power adapter supplied with the product.
- Do not overload wall outlet or extension cords as this may increase the risk of electric shock or fire. If the power cord is frayed, replace it with a new one.
- Proper ventilation is necessary to prevent the product overheating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation. It is recommended to mount the product with a stack.
- Do not place the product near any source of heat or expose it to direct sunlight.
- Do not expose the product to moisture. Never spill any liquid on the product.
- Do not attempt to connect with any computer accessory or electronic product without instructions from qualified service personnel. This may result in risk of electronic shock or fire.
- Do not place this product on unstable stand or table.

9.1.2 For Using

- Power off and unplug this product from the wall outlet when it is not in use or before cleaning. Pay attention to the temperature of the power adapter. The temperature might be high.
- After powering off the product, power on the product at least 15 seconds later.
- Do not block the ventilating openings of this product.
- When the product is expected to be not in use for a period of time, unplug the power cord of the product to prevent it from the damage of storm or sudden increases in rating.

9.1.3 For Service

Do not attempt to disassemble or open covers of this unit by yourself.
Contact qualified service personnel under the following conditions:

- If the power cord or plug is damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally when the operating instructions are followed.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in performance.

9.1.4 Warning

- This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person’s body (excluding extremities of hands, wrist and feet) during wireless modes of operation.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2)

this device must accept any interference received, including interference that may cause undesired operation.

9.1.5 Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

10.Certifications

FCC

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless Innoband expressly approves the changes or modifications.

Warning: Operation is subject to the following two conditions:
1) This device may not cause harmful interference.
2) This device must accept any interference received including interference that may cause undesired operation.

FCC Part 68 Notice

This equipment complies with Part 68 of FCC Rules. On the base unit of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. IF REQUESTED, THIS INFORMATION MUST BE GIVEN TO THE TELEPHONE COMPANY.
The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.
If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.
Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.
If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.
The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.
This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

NOTICE: The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or an electronic device to send any message via a telephone fax machine, unless such a message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission the following information:

- ✓ The date and time of transmission
- ✓ Identification of either business, business entity or individual sending message
- ✓ Telephone number of either the sending machine, business entity or individual

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate.
Do not use any other power adapter except the one that accompanies the unit. Use of other adapter could result in damage to the unit. To prevent electronic shock, please do not open the cover.

11.Warranty

Innoband warrants that equipment furnished will be free from defects in material and workmanship for a period of one year from the confirmed date of purchase of the product new from the retail location. Upon written notice of any such defect, the manufacturer will, at its option, repair or replace the defective item under the terms of this warranty, subject to the provisions and specific exclusions listed herein.

This warranty shall not apply to equipment that has been previously repaired or altered outside our facilities in any way, nor will it apply if the equipment has been used in a manner exceeding its specifications or if the serial number has been removed.

We do not assume liability for consequential damages as a result from our product use, and in any event our liability shall not exceed the original selling price of the equipment.

The equipment warranty of Innoband Technologies, Inc. shall constitute the sole and exclusive remedy of any Buyer of the manufacturer's equipment and the sole and exclusive liability of the manufacturer, its successors or assigns, in connection with equipment purchase and in lieu of all other warranties expressed, implied or statutory, including, but not limited to, any implied warranty of merchantability or fitness and all other obligations or liabilities of the manufacturer, its successors, or assigns.

Fill out the next page and mail or fax to Innoband Technologies, Inc. for product registration.

Registration Card

Innoband 6012-B1 Product Registration	
Name:	
Company:	
Address:	
City/State/Zip:	
Phone:	
E-mail:	
Serial Number:	
Purchased from:	
Date of Purchase:	

Please cut out the above Product Registration Card and send in with a self-addressed stamped envelope to:

Innoband Technologies, Inc.
2526 Qume Dr. Ste 21
San Jose, CA 95131

ATTN: Customer Service

12.Contact information

We would more than love to help if you have further technical questions, please visit our Website at http://www.innoband.com or send E-mail to support@innoband.com

Company Address
Innoband Technologies, Inc
2526 Qume Dr. Ste 21
San Jose, CA 95131